Università degli Studi di Pavia – Università degli Studi di Milano-Bicocca

DIPARTIMENTO DI MATEMATICA
Corso di Dottorato di Ricerca consortile in Matematica

Tesi di Dottorato di Ricerca

Just infiniteness and other properties of the generalized Nottingham group

Autore:
Davide Veronelli

Relatore:
Prof. Thomas S. Weigel

Dicembre 2019

A Simone
Per i bellissimi anni passati

A Enea
e chi verrà
Per i promettenti anni a venire

Contents

Introduction **iv**

I The generalized Nottingham group over arbitrary rings **1**

1 Introducing the Nottingham group **2**

1.1 The algebra of formal power series 2

1.1.1 Algebra and total algebra over a ring 2

1.1.2 The free commutative monoid 3

1.1.3 Polynomial ring and formal power series algebra 4

1.2 Substitution and endomorphisms 5

1.2.1 Separation Lemma 6

1.3 Automorphisms 7

1.4 Group of formal power series n-tuples under substitution 8

1.4.1 Basic computations 10

1.5 Topology 13

2 The associated Lie algebra **16**

2.1 Derivation algebra 16

2.2 N-series and Lie rings 18

2.3 The Lie ring associated to the generalized Nottingham group 20

II Cartan type and other subgroups **23**

3 Cartan type subgroups **24**

3.1 The exterior algebra of differential forms 24

3.2 The Special subgroup over a finite field 26

4 Pseudo-algebraic subgroups **29**

4.1 Basic introduction to linear algebraic groups 29

4.2 Definition 31

4.3 Functoriality of pseudo-algebraic groups 32

4.4 Lie rings of pseudo-algebraic groups 35

5 Other subgroups **37**
5.1 Subgroups related to ideals 37
5.2 Index-subgroups 39
5.2.1 Hausdorff spectrum of the Nottingham group 41

III The generalized Nottingham group over a finite field **45**

6 Just infiniteness of the Nottingham group **46**
6.1 Technical notation and visual representation 47
6.2 Basic stages of the proof 50
6.3 Actual proof 57
6.4 Quantitative version of Theorem 0.2 59

7 Abstract randomly generated subgroups **62**
7.1 Probabilistic identities 62
7.2 Proof of the theorem 63

8 Conclusions **66**

Appendices **69**

A Inverse limits **70**

B Combinatorial computations **72**

C Miscellanea **76**

Introduction

A profinite group is said to be just infinite (j. i.) if it is infinite and every non-trivial closed normal subgroup is open, while it is said hereditarily just infinite (h. j. i.) if every open subgroup is just infinite. Just infinite groups play a role in profinite group theory analogous to that of simple groups in finite group theory. For example, every finitely generated pro-p group has a just infinite quotient, so problems about pro-p groups may be reduced to problems about just infinite groups, more or less like finite groups problems may be reduced to simple groups.

An other interest in (pro-p) just infinite groups is in coclass theory. In a paper from 1980, C. R. Leedham-Green and M. F. Newman [28] started a project to roughly classify finite p-groups somehow using their coclass (i. e. given a p-group of order p^n, the difference between n and its class), stating some conjectures that involved pro-p groups. These conjectures were later proved in several papers ([27], [26], [13], [37], [23], [24], [36]) and research in this area revealed the increasing interest in just infinite groups. The reader is pointed to [35] for a more detailed review on the subject. A minor remark should be done here: in this context, we are mostly interested in profinite groups of finite width.

Despite the importance of just infinite groups, a little is known about them. Exploiting a well known paper by J. S. Wilson [43], it was shown by R. I. Grigorchuk [19] that any just infinite profinite group either is a branch group or contains an open normal subgroup isomorphic to the direct product of finite copies of an hereditarily just infinite group. This result is called Wilson's dichotomy. Thus, in studying just infinite profinite groups, we actually reduce to branch groups and h. j. i. groups.

However things here become even more unclear. In particular, despite decades of research on h. j. i. groups, we even lack examples. Actually, here it is the — short — full list of known classes of h. j. i. profinite groups.

- The group of p-adic integers and some finite extensions. Indeed it is easy to observe that a virtually abelian h. j. i. group must be a finite extension of $\mathbb{Z}_p$.
- Hereditarily just infinite groups of Lie type. Let $\mathbb{G}$ be an absolutely simple simply connected algebraic group defined over a local field F. Then any open compact subgroup G of $\mathbb{G}(F)$ whose intersection with the center of $\mathbb{G}(F)$ is trivial is h. j. i. and it is said to have Lie type [2]. This is a consequence of a well known result by R. Pink [29].
- Wilson's groups. These are groups built taking inverse limits of iterated wreath product of simple groups. They were first introduced by J. S. Wilson [44] and generalized by M. Vannacci [40]. So far, they are the unique known examples of h. j. i. profinite groups that are not virtually pro-p.
- The Nottingham group and some classes of subgroups. Actually, because of a celebrated result by R. Camina [10], all pro-p just infinite groups are isomorphic to some closed subgroup of the Nottingham group, thus it does not really make sense to speak about a

category of h. j. i. groups that are subgroups of the Nottingham group. However, here we mean groups which have a natural construction as subgroups of the Nottingham group and do not belong to the other categories. Groups in this family are said to have Nottingham type [2]. More details about this class will be given later.

From this list the reader might have noticed an other reason of interest in h. j. i. groups: they are apparently always rather amazing groups on their own. Indeed, whereas the first two categories are completely classical and well known, the other two are — on the other side — somewhat exceptional, in many ways. Thus, for example, they have a similar — very strong — embedding property. We have already mentioned the result by Camina [10]: the full statement says that every countably based pro-p group is isomorphic to a closed subgroup of the Nottingham group. Similarly, some Wilson groups contain a closed embedding of any countably based profinite group [44]. So these groups are in some sense small, as every proper continuous image of every open subgroup is finite, but on the other hand they are very large, in that they contain entire categories of groups.

So, starting from middle '00s, intensive investigations have been done about h. j. i. groups. The earliest works aimed to find new examples among closed subgroups of the Nottingham group, the most remarkable of which may be those introduced by I. Fesenko [18], Y. Barnea and B. Klopsch [3] (see Section 5.2) and M. Ershov [14]. Then there have been also more abstract result: characterizations (for example qualitative [32] and quantitative [30, 31] characterizations by C. D. Reid) and even a full — although quite rough — classification. In fact, in a paper published in 2011 [2], Y. Barnea, M. Ershov and T. S. Weigel obtained a complete classification in four classes of h. j. i. groups through their abstract commensurator.

This is more or less the motivating context to investigate a generalization of the Nottingham group. Before diving into the main subject of this thesis, it might be worth to spend some words about the "classic" (not generalized) Nottingham group.

The Nottingham group may be defined in different ways. It is so called because of the first appearance in the context of group theory due to D. L. Johnson [21] and his PhD student I. O. York [45] from the University of Nottingham. They defined it as the group of formal power series over a commutative ring R of the form $t(1 + tf)$ — where f is any formal power series in $R[\![t]\!]$ — under substitution. However the most interesting cases appear when R is a finite field and in such a form it was already known in number theory to be the group of *wild* automorphisms of the field $\mathbb{F}_q((t))$ of Laurent series over the finite field $\mathbb{F}_q$ of order q. Details are skipped as this are particular cases of definitions and results given in Chapter 1; for a specific overview on the classic Nottingham group, the reader may want to look at [11]. Few computations show that the Nottingham group over a finite field of odd characteristic is an h. j. i. pro-p group and Hegedűs [20] proved that the same holds also when the field characteristic is 2. The interest in the Nottingham group considerably increased after the already mentioned Camina's result about the embedding of countably based pro-p groups was published. Since then it has been subject of intensive investigations in different fields, as this last property makes of the Nottingham group the perfect test-group for conjectures, especially — but not exclusively — about pro-p groups (an example in this direction is given in Chapter 7). Other results about the Nottingham group have been proved: it is finitely presented [16]; if the field has order p and p is at least 5, then its automorphism group coincides with the automorphism group of $\mathbb{F}_p[\![t]\!]$ [22] and with its commensurator group [15].

In 1995, before Wilson's dichotomy was explicitly proved and therefore before the major interest in h. j. i. groups, aiming to find new examples of just infinite groups, A. Shalev [34] informally presented a joint work with C. R. Leedham-Green that introduced the so-called Cartan type groups. These will be precisely defined in Chapter 3; so far, it is enough to know that they are particular closed subgroups of a somewhat natural generalization of the Nottingham group.

Indeed, the Nottingham group over $\mathbb{F}_p$ can also be defined as the group of automorphisms of $\mathbb{F}_p[\![t]\!]$ that induce identity on $\mathbb{F}_p[\![t]\!]/(t^2)$ [25]. Thus we can easily generalize it to automorphisms of $\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ that induce identity modulo $(t_1^2, t_1t_2, t_2^2, \dots, t_n^2)$. Actually, the ring $\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ has a natural filtration of characteristic ideals $\{\mathfrak{m}^i\}_{i\in\mathbb{N}}$ — namely the set of elements of order at least i — and we define $\mathrm{Aut}^i_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ to be the group of automorphisms of $\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ that induce the identity modulo $\mathfrak{m}^{i+1}$. In this notation the generalized Nottingham group of rank n over $\mathbb{F}_p$ is the group $\mathrm{Aut}^1_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]$. Such a group has a natural topology that turns it into a pro-p group.

The feeling was that Cartan-type groups might be just infinite and Shalev even stated the following theorem.

Theorem 0.1 (Theorem 8.5 [34])**.** *When $n > 1$:*

(i) $\{\mathrm{Aut}^i_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]\}_{i\in\mathbb{N}}$ *coincides with the lower central series of* $\mathrm{Aut}^1_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]$*;*

(ii) $\mathrm{Aut}^1_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ *is finitely generated by* $n \times \binom{n+1}{n-1}$ *elements;*

(iii) each quotient $\mathrm{Aut}^i_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]/\mathrm{Aut}^{i+1}_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ *is elementary abelian of rank* $n \times \binom{n+i}{n-1}$*;*

(iv) $\mathrm{Aut}^1_{\mathbb{F}_p}\mathbb{F}_p[\![t_1, \dots, t_n]\!]$ *is just infinite.*

It is worth to say something more about this theorem. First of all, the hypothesis $n > 1$ is necessary only for the first statement, whereas all other assertions are true for the classic Nottingham group ($n = 1$). Parts (*i*) and (*iii*) imply that the generalized Nottingham group has infinite width. We already mentioned the width of a profinite group G: this is defined to be $\sup_{i\geq 1} |\gamma_i(G) : \gamma_{i+1}(G)|$ where $\{\gamma_i(G)\}$ denotes the lower central series of G. Being of infinite width makes the generalized Nottingham group ($n > 1$) less interesting in the coclass theory context, but on the other hand it means that it is sensibly larger — in some sense — than the classic Nottingham group, stressing the double nature (small and large) of these kind of groups. Actually, as far as we know, it is the first example of (hereditarily) just infinite pro-p group of infinite width. Finally, the fourth statement is not so simple to prove as for the classic Nottingham group and it also sounds a little weak nowadays, in that we are now more interested in knowing whether it is hereditarily just infinite or not.

However the proof of Theorem 0.1 was not published and Shalev himself warned to be careful on these results as they were “not fully written up yet”. Nearly 25 years have passed since then and still neither a proof nor even precise definitions of all these concepts have been published, although Cartan-type profinite groups have often been considered a class of h. j. i. groups in literature [5].

This thesis aims to partially fill such a gap. In particular we are going to define the generalized Nottingham group over arbitrary rings and to prove its principal properties, among which points (*i*), (*ii*) and (*iii*) of Shalev's Theorem (Chapter 1). Concerning just infiniteness, we are going to prove the following theorem.

Theorem 0.2. *The generalized Nottingham group over a finite field of odd characteristic is hereditarily just infinite.*

This is a stronger version of the fourth assertion of Theorem 0.1. The restriction to odd characteristic may not surprise the reader. Our guess is that also in characteristic 2 the generalized Nottingham group may be h. j. i., but as for the classic case, the proof might be completely different.

In the meanwhile we give a — possible — precise definition of Cartan-type groups (Chapter 3) and we introduce other families of subgroups that might have some interest (Chapter 4 and Chapter 5). In particular, using a result of Barnea and Klopsch for the classic Nottingham group [3], in Section 5.2 we will be able to exhibit a non-trivial subset of the Hausdorff spectrum of the generalized Nottingham group over a finite field of odd characteristic, which is profinite. The Hausdorff dimension was originally defined for Euclidean spaces, to study fractal subspaces. However its definition can be easily extended to any metric space, in particular A. Abercrombie [1] introduced it in the word of profinite groups, where it fits very well since these are intrinsically fractal, being compact and totally disconnected. The Hausdorff spectrum is the set of all possible Hausdorff dimensions of subgroups with respect to some particular metric on the group. For further details about the Hausdorff dimension, the reader is pointed to [35], [4] (in the profinite context) and [17] (in the original setting).

Finally, in Chapter 7 we also prove a result in the context of probabilistic identities, namely that k randomly chosen elements of the generalized Nottingham group generate a free abstract subgroup of rank k.

Acknowledgement. I must thank my supervisor Prof. Thomas S. Weigel, for having introduced to me the main topic of this thesis and for the good suggestions to improve it. I would like to thank also Prof. Benjamin Klopsch: the problem faced in Chapter 7 was brought to my attention by him and solved while I was visiting him at HHU in Düsseldorf. He also suggested me to extend index-subgroups to the generalized case to deal with the Hausdorff spectrum (see Section 5.2). Finally, I thank both Benjamin Klopsch himself and Jon González Sánchez for the patient and careful corrections and suggestions to the preliminary versions of this thesis.

Notation 1. The letters $\mathbb{Z}$, $\mathbb{N}_0$, $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{R}$ respectively stand for sets of integer numbers, non-negative integers, positive integers, rational numbers, real numbers. Whenever p is a prime $\mathbb{Z}_p$ denotes the ring of p-adic integers, while for any power q of p, the symbol $\mathbb{F}_q$ denotes the finite field of order q.

Notation 2. Rings — unless otherwise explicitly stated — are meant to be Hausdorff topological unitary and commutative rings. Thus in particular a ring morphism is continuous and preserves the unity. In this same perspective, an ideal is the kernel of a (continuous) morphism, that is an abstract ideal which is topologically closed. Note that requiring an Hausdorff topology for R is just a mild restriction, as every ring can be considered a discrete topological ring and any morphism between discrete ring is continuous; on the other side, if we endow R with a more sophisticated topology, we gain some structures that might be useful. Thus it sounds very reasonable to consider every ring a topological ring. As for other structures, such as topological groups, when we want to temporarily forget the topological structure, we speak of *abstract* rings (subrings, ideals, morphism,...).

Given a ring (in our meaning) R, the category of R-algebras is the coslice category of rings with respect to R. In other words an R-algebra is a ring A endowed with a ring morphism $R \to A$ and a morphism $\rho : A \to B$ of R-algebras $\alpha : R \to A$ and $\beta : R \to B$ is a ring morphism such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "\rho"] & & B \\
& R \arrow[ul, "\alpha"] \arrow[ur, "\beta"'] &
\end{tikzcd}$$

commutes. It follows that R-algebras are commutative, associative and unitary.

A remarkable exception to this notational rule about rings is for Lie rings. These are meant to be $\mathbb{Z}$-modules endowed with a binary $\mathbb{Z}$-bilinear operation [,] — called *Lie brackets* operation —

that satisfies $[x, x] = 0$ and $[[x, y], z] + [[y, z], x] + [[z, x], y] = 0$ (Jacobi identity) for all elements x, y and z of the Lie ring. Finally, as an R-algebra is a ring with the additional structure of R-module — this is completely equivalent to our definition of R-algebra — similarly a Lie R-algebra is a Lie ring with the additional structure of R-module, with respect to which Lie brackets are R-bilinear.

Notation 3. Let R be any ring and let n be a positive integer. Then $\mathrm{GL}_n(R)$ denotes the general linear group over R, that is the group of matrices $n \times n$ with coefficients in R that are invertible, that is whose determinant is invertible in R, while $\mathrm{SL}_n(R)$ denotes the special linear group over R, that is the subgroup of $\mathrm{GL}_n(R)$ whose matrices have determinant 1.

Notation 4. Monoid and group product (so in particular composition of endomorphisms), ring multiplication and scalar product (when dealing with modules) will usually be denoted by juxtapposition of factors, with no sign. However, a plus sign $(+)$ is most often used for intrinsically commutative operations (sums in rings, group operation of modules). A dot $(\cdot)$ will be used to mark matrix multiplication, whereas a circle $(\circ)$ denotes the operation of substitution introduced in Chapter 1.

Notation 5. For every structure with an underlying set A and for every ring R, the Kronecker delta function on A to R is the function from $A \times A$ to R that maps (a, b) to $\delta_{a,b}$ that — for every $a, b \in A$ — is the identity of R if $b = a$, otherwise it is $0 \in R$.

Part I

The generalized Nottingham group over arbitrary rings

Chapter 1

Introducing the generalized Nottingham group

In this chapter we give the first definitions and properties of the group of automorphisms of $R[\![\boldsymbol{t}]\!]$ (actually a subgroup of it, in general) and of the generalized Nottingham group. To start with, we recall some theory about the ring of formal power series ([7], [8], [33] are used).

1.1 The algebra of formal power series

The main reference for this section is Bourbaki [8, 7].

1.1.1 Algebra and total algebra over a ring

Let R and M be a commutative ring and a commutative (additive) monoid respectively. The support of a sequence $(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in M} \in R^M$ is defined to be the set $\mathrm{Supp}(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in M}$ of elements $\boldsymbol{\alpha} \in M$ such that $a_{\boldsymbol{\alpha}}$ is not the zero element of R. The algebra of M over R is defined to be the R-algebra $R[M]$ of finitely supported sequences $(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in M} \in R^M$ under component-wise addition and product given by

$$(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in M}(b_{\boldsymbol{\beta}})_{\boldsymbol{\beta}\in M} = \left(c_{\boldsymbol{\gamma}} = \sum_{\boldsymbol{\alpha}+\boldsymbol{\beta}=\boldsymbol{\gamma}} a_{\boldsymbol{\alpha}} b_{\boldsymbol{\beta}}\right)_{\boldsymbol{\gamma}\in M} ; \tag{1.1}$$

see [8].

If we furthermore assume that for any $\boldsymbol{\gamma} \in M$ there are finitely many pairs $(\boldsymbol{\alpha}, \boldsymbol{\beta}) \in M \times M$ such that $\boldsymbol{\alpha} + \boldsymbol{\beta} = \boldsymbol{\gamma}$, we can also define the total algebra $R[\![M]\!]$ of M over R in the same way, allowing infinitely supported sequences.

Of course we have a natural embedding of $R[M]$ into $R[\![M]\!]$, that allows us to use the same conventions for both algebras. We usually write elements of these algebras as formal series, adopting

$$\sum_{\boldsymbol{\alpha}\in M} a_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}} \tag{1.2}$$

for the sequence $(a_{\boldsymbol{\alpha}})_{\boldsymbol{\alpha}\in M}$. We may also omit summand whose coefficient is $0 \in R$, using for example $\boldsymbol{t}^{\boldsymbol{\alpha}}$ to denote the element $(\delta_{\boldsymbol{\alpha},\boldsymbol{\beta}})_{\boldsymbol{\beta}\in M}$, where $\delta_{\boldsymbol{\alpha},\boldsymbol{\beta}}$ is the Kronecker delta function on M

to R. The zero element — usually simply denoted by 0 — in both these algebras is given by $\sum_{\boldsymbol{\alpha}\in M} 0\boldsymbol{t}^{\boldsymbol{\alpha}}$, while the identity — denoted by 1 — is $\boldsymbol{t}^0$.

Since the total algebra $R[\![M]\!]$, from a set-theoretic point of view, is exactly $R^M = \prod_{\boldsymbol{\alpha}\in M} R\boldsymbol{t}^{\boldsymbol{\alpha}}$, when R is a topological group it may be endowed with the product topology. Then $(R[\![M]\!], +)$ is the product of topological groups and so it is itself a topological group. The product is also continuous, as in each component is given by formula (1.1) that is a polynomial function over the topological ring R. Thus $R[\![M]\!]$ is a topological ring, as well as $R[M]$ endowed with the subspace topology. Actually $R[M]$ is a dense subspace of $R[\![M]\!]$.

Note that since R is Hausdorff, so it is $R[\![M]\!]$ and, by Tychonoff's Theorem, if R is compact then so it is $R[\![M]\!]$.

Finally, the following proposition is an easy exercise.

Proposition 1.1. *Let G be a set of generators of M. Then $\{\boldsymbol{t}^{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in G\}$ generate (both abstractly and topologically) $R[M]$ and topologically generate $R[\![M]\!]$.*

By "topological" generation, we mean that the coarsest closed set containing the algebra generated by G is $R[\![M]\!]$ itself.

1.1.2 The free commutative monoid

Let n be a positive integer, consider the free abelian group F over a set of cardinality n and choose a family of generators $\{\boldsymbol{\epsilon}_1, \dots, \boldsymbol{\epsilon}_n\}$. Using the additive notation, any $\boldsymbol{\alpha} \in F$ can be uniquely written as a finite sum of generators:

$$\boldsymbol{\alpha} = \sum_{i=1}^{n} \alpha_i \boldsymbol{\epsilon}_i$$

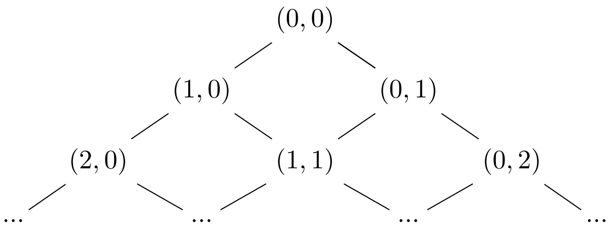
where each α_i is an integer. The word length of $\boldsymbol{\alpha}$ is called weight and denoted by $|\boldsymbol{\alpha}|$, that is

$$|\boldsymbol{\alpha}| = \sum_{i=1}^{n} |\alpha_i|.$$

Of course we may identify the free commutative group with $\mathbb{Z}^n$ and we may also consider it as a poset by imposing $\boldsymbol{\alpha} \leq \boldsymbol{\beta}$ — for every $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^n$ and $\boldsymbol{\beta} = (\beta_i)_{i=1}^n$ in $\mathbb{Z}^n$ — if and only if $\alpha_i \leq \beta_i$ for every $i \in \{1, \dots, n\}$. Such a poset is indeed a lattice, where the infimum and the supremum of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are $(\min\{\alpha_i, \beta_i\})_{i=1}^n$ and $(\max\{\alpha_i, \beta_i\})_{i=1}^n$ respectively. This lattice can be effectively represented by the Cayley graph of F.

We will mostly work with the submonoid generated by $\{\boldsymbol{\epsilon}_1, \dots, \boldsymbol{\epsilon}_n\}$, denoted by ${\mathbb{N}_0}^n$ that is also a lattice.

Example 1.1. When $n = 2$, the Cayley graph of ${\mathbb{N}_0}^n$ is represented by



where each level (horizontal line) is associated to a particular weight. Though very simple, this graph will turn out to be incredibly useful later on and it is worth to be represented.

Notation 6. From now on, bold lowercase Greek letters (especially the first ones occurring in the alphabet: $\boldsymbol{\alpha}$, $\boldsymbol{\beta}$, $\boldsymbol{\gamma}, \ldots$) are reserved for elements of ${\mathbb{N}_0}^n$.

Lemma 1.2. *Let j be a positive integer. The number of elements in ${\mathbb{N}_0}^n$ whose weight is j is $\binom{j+n-1}{n-1}$*

Proof. Consider the set $\{1, \ldots, j+n-1\}$. There is a one-to-one correspondence between the subsets of cardinality $n-1$ of such a set and the n-tuples of non-negative integers whose sum is j. Essentially a subset $\{a_1 < a_2 < \ldots < a_{n-1}\}$ is associated to $(a_i - a_{i-1} - 1)_{i=1}^n \in {\mathbb{N}_0}^n$ where we set $a_0 = 0$ and $a_n = j+n$. Such subsets are exactly $\binom{j+n-1}{n-1}$. □

1.1.3 Polynomial ring and formal power series algebra

By definition (compare [7]) the ring of polynomials in n indeterminates over R is the algebra of ${\mathbb{N}_0}^n$ over R, whereas the ring of formal power series in n indeterminates over R is the total algebra of ${\mathbb{N}_0}^n$ over R. When no ambiguity occurs, we denote them with $R[\boldsymbol{t}]$ and $R[\![\boldsymbol{t}]\!]$ instead of $R[{\mathbb{N}_0}^n]$ and $R[\![{\mathbb{N}_0}^n]\!]$ respectively.

As already noticed, the algebra $R[\![\boldsymbol{t}]\!]$ is Hausdorff and also compact if so it is R.

By Proposition 1.1, the algebra $R[\![\boldsymbol{t}]\!]$ is topologically generated by $\{t_1 := \boldsymbol{t}^{\epsilon_1}, \ldots, t_n := \boldsymbol{t}^{\epsilon_n}\}$. Let $\mathfrak{m}$ denote the abstract ideal generated by $t_1, \ldots, t_n$. and for every $i \in \mathbb{N}$ define $\mathfrak{m}^i$ to be the *abstract* ideal generated by the set $\{xy \mid x \in \mathfrak{m},\ y \in \mathfrak{m}^{i-1}\}$ where we impose $\mathfrak{m}^0$ to be the entire ring $R[\![\boldsymbol{t}]\!]$. Note that $\mathfrak{m}^1 = \mathfrak{m}$. Any endomorphism ϕ of $R[\![\boldsymbol{t}]\!]$ that preserves $\mathfrak{m}$ preserves also each $\mathfrak{m}^i$, since they are constructed as "verbal" subideals. Moreover, each $\mathfrak{m}^i$ can also be described as the set of formal power series $f \in R[\![\boldsymbol{t}]\!]$ of the form $\sum_{|\boldsymbol{\alpha}| \geq i} f_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}}$. So, seen as a subset of $R^{{\mathbb{N}_0}^n} = \prod_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} R\boldsymbol{t}^{\boldsymbol{\alpha}}$, it is $\prod_{|\boldsymbol{\alpha}|<i} \{0\} \times \prod_{|\boldsymbol{\alpha}| \geq i} R$ that is closed, being the product of closed subsets of R. So in particular all these abstract ideals are indeed *topological* ideals.

Definition. The order of $f \in R[\![\boldsymbol{t}]\!] \setminus \{0\}$ is defined to be

$$\operatorname{ord}(f) := \max\left\{i \mid f \in \mathfrak{m}^i\right\},$$

whereas the order of $0 \in R[\![\boldsymbol{t}]\!]$ is canonically set to infinity.

Note that the order of a formal power series $f = \sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}}$ equals $\min\{|\boldsymbol{\alpha}| \mid f_{\boldsymbol{\alpha}} \neq 0\}$, hence we may infer the following lemma, whose exact proof is an easy — and well known — exercise.

Lemma 1.3. *Let f and g be in $R[\![\boldsymbol{t}]\!]$. Then* $\operatorname{ord}(f+g) \geq \min\{\operatorname{ord}(g), \operatorname{ord}(f)\}$ *(and if equality do not hold then* $\operatorname{ord}(g) = \operatorname{ord}(f)$ *and $f \equiv -g$ modulo $\mathfrak{m}^{\operatorname{ord}(f+g)}$) and* $\operatorname{ord}(fg) \geq \operatorname{ord}(f) + \operatorname{ord}(g)$ *(and equality always holds if R is a domain).*

Looking at the topological space of $R[\![\boldsymbol{t}]\!]$ as the product $\prod_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} R\boldsymbol{t}^{\boldsymbol{\alpha}}$ we have that, given a base for the neighbourhoods $\mathcal{U}$ of $0 \in R$, a base for the neighbourhoods of $0 \in R[\![\boldsymbol{t}]\!]$ is given by sets of the form

$$U = \prod_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} U_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}},$$

where $U_{\boldsymbol{\alpha}} \in \mathcal{U}$ for every $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$ and $U_{\boldsymbol{\alpha}} = R$ but for finitely many $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$. The finiteness condition on n-tuples $\boldsymbol{\alpha}$ such that $U_{\boldsymbol{\alpha}}$ is a proper subset of R implies there exists $i \in \mathbb{N}_0$ such that $U_{\boldsymbol{\alpha}} = R$ for every $\boldsymbol{\alpha}$ of weight greater than i, that is U contains $\mathfrak{m}^{i+1}$. In particular, if R is discrete then the family of ideals $\{\mathfrak{m}^i\}_{i \in \mathbb{N}}$ forms a base for the neighbourhoods of 0, while if R is not discrete $\mathfrak{m}^i$ is not open for any $i \in \mathbb{N}$.

Proposition 1.4. *The algebra $R[\![\boldsymbol{t}]\!]$ is isomorphic to the inverse limit $\varprojlim_{i\in\mathbb{N}} R[\![\boldsymbol{t}]\!]/\mathfrak{m}^i$.*

Proof. The statement can be easily checked in many ways. For example one might show that $R[\![\boldsymbol{t}]\!]$ is homeomorphic to the usual construction (see [33] and (A.1)) of inverse limit. □

1.2 Substitution and endomorphisms

Let us temporarily assume that R is discrete. We have already observed that $R[\![\boldsymbol{t}]\!]$ is topologically generated by $t_1, \dots, t_n$ as R-algebra and therefore a continuous R-endomorphism is completely determined by the images of the indeterminates. Moreover, since, for every $i \in \{1, \dots, n\}$, the sequence $({t_i}^j)$ converges to 0 as j tends to infinity, the images of $t_1, \dots, t_n$ must have the same property. By [7, Chapter IV, §4, Proposition 4], this is actually the unique condition, that is, for every n-tuple $\boldsymbol{x} = (x_i)_{i=1}^n$ of elements in $R[\![\boldsymbol{t}]\!]$ such that ${x_i}^j$ tends to 0 as j tends to infinity, the map $\Phi_{\boldsymbol{x}}$ from $R[\![\boldsymbol{t}]\!]$ to itself, sending $f \in R[\![\boldsymbol{t}]\!]$ to $f \circ \boldsymbol{x} \in R[\![\boldsymbol{t}]\!]$ — where $f \circ \boldsymbol{x}$ denotes the formal power series f where we replace x_i to t_i for every $i \in \{1, \dots, n\}$ — is a continuous R-endomorphism.

Let $\boldsymbol{x} = (x_i)_{i=1}^n$ and $\boldsymbol{y} = (y_i)_{i=1}^n$ be two n-tuples satisfying the convergence hypothesis and let $\Phi_{\boldsymbol{x}}$ and $\Phi_{\boldsymbol{y}}$ be the associated endomorphisms, namely the endomorphisms that for every $i \in \{1, \dots, n\}$ map t_i to x_i and t_i to y_i respectively. Then, for every $i \in \{1, \dots, n\}$

$$\Phi_{\boldsymbol{y}}(\Phi_{\boldsymbol{x}}(t_i)) = \Phi_{\boldsymbol{y}}(x_i) = x_i \circ \boldsymbol{y}$$

and so the n-tuple associated to $\Phi_{\boldsymbol{y}}\Phi_{\boldsymbol{x}}$ is $(x_i \circ \boldsymbol{y})_{i=1}^n$, that will be denoted by $\boldsymbol{x} \circ \boldsymbol{y}$. In other words we obtained the following result.

Lemma 1.5. *The set of n-tuples in $(R[\![\boldsymbol{t}]\!])^n$ that satisfy the previously mentioned convergence property form a monoid under the operation $\circ$ (called substitution) anti-isomorphic to the set $\mathrm{End}_R R[\![\boldsymbol{t}]\!]$ of continuous R-endomorphisms under composition.*

Restricting this lemma to endomorphisms that preserve $\mathfrak{m}$ — i. e. whose image of $\mathfrak{m}$ is a subset of $\mathfrak{m}$ itself — we obtain a further refinement.

Proposition 1.6. *The monoid of $\mathfrak{m}$-preserving continuous endomorphisms of $R[\![\boldsymbol{t}]\!]$ under composition is anti-isomorphic to the monoid of n-tuples $(x_i)_{i=1}^n$ in the direct product of $R[\![\boldsymbol{t}]\!]$ with itself n times such that $x_i \in \mathfrak{m}$ for every $i \in \{1, \dots, n\}$, under substitution.*

Now we may want to leave the assumption on the discrete topology of R, as in general we are interested also in different topologies. We shall recover generality from the next proposition, but, before that, let us introduce some new notation.

Notation 7. The just mentioned set of n-tuples of elements in $\mathfrak{m}$ is denoted by $\mathcal{M}_n(R)$. Moreover, for every $i \in \mathbb{N}$, we define $\mathcal{M}_n^i(R)$ to be the set of n-tuples whose components are in $\mathfrak{m}^i$ (so that $\mathcal{M}_n(R) = \mathcal{M}_n^1(R)$). The monoid of *abstract* $\mathfrak{m}$-preserving R-endomorphisms of $R[\![\boldsymbol{t}]\!]$ is denoted by $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$.

Remark 1.7. Note that each $\mathcal{M}_n^i(R)$ is a (closed) ideal of $(R[\![\boldsymbol{t}]\!])^n$ — being the direct product of $\mathfrak{m}^i$ with itself n times — and the topological ring $(R[\![\boldsymbol{t}]\!])^n$ is isomorphic to the inverse limit $\varprojlim (R[\![\boldsymbol{t}]\!])^n/\mathcal{M}_n^i(R)$, being the direct product of inverse limits.

Proposition 1.8. *Let R be any topological ring. Every $\phi \in \mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is continuous.*

To prove this proposition we need the following lemma.

Lemma 1.9. *Let V and W be free R-modules of finite rank endowed with the product topology. Then every R-linear morphism $\phi : V \to W$ is continuous.*

Proof. Let $\{\boldsymbol{w}_j \mid 1 \leq j \leq s\}$ and $\{\boldsymbol{e}_j \mid 1 \leq j \leq r\}$ be bases for W and V respectively. For every R-morphism $\phi : V \to W$ and every $\boldsymbol{v} = \sum_{i=1}^{r} v_i \boldsymbol{e}_i$ in V, we have $\phi(\boldsymbol{v}) = \sum_{i=1}^{r} v_i \phi(\boldsymbol{e}_i)$ where in turn each image of $\boldsymbol{e}_i$ is of the form $\sum_{j=1}^{s} a_{ij} \boldsymbol{w}_j$ for some $(a_{ij})_{i=1,j=1}^{r\ \ s} \in R^{r\times s}$. Thus $\phi(\boldsymbol{v}) = \sum_{j=1}^{s} \left(\sum_{i=1}^{r} a_{ij}\right) \boldsymbol{w}_j$. As on W we have the product topology, the endomorphism ϕ is continuous if and only if its composition with the projection on each component is continuous, i. e. if and only if the map that maps $(a_{ij})_{i=1}^{r}$ to $\sum_{i=1}^{r} a_{ij}$ is continuous. But this is clearly true, since R is a topological ring. □

Proof of Proposition 1.8. As for every $i \in \mathbb{N}_0$, the ideal $\mathfrak{m}^{i+1}$ is preserved by $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$, we are allowed to define a monoid morphism

$$\tilde{\chi}_i : \operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \to \operatorname{End}_R(R[\![\boldsymbol{t}]\!]/\mathfrak{m}^{i+1}) \tag{1.3}$$

sending each $\phi \in \operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ to the endomorphism $\tilde{\chi}_i(\phi) \in \operatorname{End}_R(R[\![\boldsymbol{t}]\!]/\mathfrak{m}^{i+1})$ that maps each equivalence class $f + \mathfrak{m}^{i+1}$ to $\phi(f) + \mathfrak{m}^{i+1}$. Then $\phi = \varprojlim \left(\tilde{\chi}_i(\phi) : R[\![\boldsymbol{t}]\!]/\mathfrak{m}^{i+1} \to R[\![\boldsymbol{t}]\!]/\mathfrak{m}^{i+1}\right)$ where each $\tilde{\chi}_i(\phi)$ is an endomorphism of an R-algebra that is free and finitely ranked as R-module and therefore, by the previous lemma, continuous. This implies that ϕ is continuous (see Remark A.2). □

So endomorphisms in $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ are continuous independently of the topology. In particular are continuous for the discrete topology on R and therefore, by Proposition 1.6, the monoid $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is anti-isomorphic to $\mathcal{M}_n(R)$ under substitution.

Remark 1.10. There are some natural assumptions over R under which $\mathfrak{m}$ is invariant under abstract (e. g. when R is a finite integral domain or it is a field) or continuous (e. g. R discrete integral domain) endomorphisms. In these cases $\{\mathfrak{m}^i \mid i \in \mathbb{N}\}$ forms a chain of closed fully characteristic (i. e. invariant under endomorphism) ideals whose intersection is trivial. Also, in these cases $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ coincides with the monoid of (abstract or continuous) endomorphisms of $R[\![\boldsymbol{t}]\!]$.

1.2.1 Separation Lemma

Lemma 1.11. *Assume R is an integral domain and let ϕ and ψ be two distinct abstract ring endomorphisms of $R[\![\boldsymbol{t}]\!]$. Then either $\phi|_{\mathfrak{m}} = \psi|_{\mathfrak{m}} = 0$, or for every $i \in \mathbb{N}$ there exists $g \in \mathfrak{m}^i$ such that $\psi(g) \neq \phi(g)$.*

Proof. First of all note that, since R is an integral domain — and therefore so it is $R[\![\boldsymbol{t}]\!]$, by Lemma 1.3 —, if there exists $k \in \mathfrak{m}$ such that $\phi(k) \neq 0$, then for every $i \in \mathbb{N}$ there exists $k_i \in \mathfrak{m}^i$ such that $\phi(k_i) \neq 0$, namely k^i. Thus we may assume that for every $i \in \mathbb{N}$ there exists $k_i \in \mathfrak{m}^i$ such that $\phi(k_i) \neq 0$. Suppose that the restrictions of ϕ and ψ to $\mathfrak{m}^i$ coincide. Then for every $h \in R[\![\boldsymbol{t}]\!]$, we have $\psi(k_i h) = \phi(k_i h)$, whence $\phi(k_i)\,(\phi(h) - \psi(h)) = 0$. As $R[\![\boldsymbol{t}]\!]$ is an integral domain, this implies that $\phi(h) = \psi(h)$ for every $h \in R[\![\boldsymbol{t}]\!]$, that is $\phi = \psi$. □

Proposition 1.12 (Separation Lemma)**.** *Let R be an integral domain and let $\{\phi_j\}_{j=1}^{r}$ ($r > 1$) be a finite family of pair-wise distinct and continuous ring endomorphisms of $R[\![\boldsymbol{t}]\!]$ that do not annihilate on $\mathfrak{m}$. Then for every open subset $A \subseteq R[\![\boldsymbol{t}]\!]$ there exists an open subset $O \subseteq A$ such that $\phi_j(O) \cap \phi_k(O) = \emptyset$ for every $1 \leq j < k \leq r$.*

Proof. We proceed by induction. First assume $r = 2$. Without loss of generality, we may assume that A is of the form

$$\{f + \sum_{\boldsymbol{\alpha}} a_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}} \mid a_{\boldsymbol{\alpha}} \in U_{\boldsymbol{\alpha}}\}, \tag{1.4}$$

where f is a formal power series in A and $\{U_{\boldsymbol{\alpha}}\}$ is a family of open neighbourhoods of 0 in R such that $U_{\boldsymbol{\alpha}} = R$ for all $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$ of weight greater than some positive integer i. In particular A contains $f + \mathfrak{m}^i$. By Lemma 1.11 there exists $g \in \mathfrak{m}^i$ such that $\phi_1(g) \neq \phi_2(g)$ and therefore if $\phi_1(f) = \phi_2(f)$ then $\phi_1(f+g) = \phi_1(f) + \phi_1(g) \neq \phi_2(f) + \phi_2(g) = \phi_2(f+g)$. Moreover if we substitute $f + g$ to f in (1.4) we obtain the same set. Thus we may assume $\phi_1(f) \neq \phi_2(f)$.

Since $R[\![\boldsymbol{t}]\!]$ is Hausdorff, we can find two open neighbourhoods U_1 and U_2 of $\phi_1(f)$ and $\phi_2(f)$ respectively whose intersection is empty. Then, since ϕ_1 and ϕ_2 are continuous, the set $A \cap \phi_1^{-1}(U_1) \cap {\phi_2}^{-1}(U_2)$ satisfies the statement.

Finally, assume $r > 2$. By inductive hypothesis, we can find a chain $A \supseteq O_1 \supseteq O_2 \supseteq O_3$ of open subsets such that $\phi_k(O_l) \cap \phi_j(O_l) = \emptyset$ for every $k \neq l$, $j \neq l$ such that $1 \leq j < k \leq r$. Then O_3 satisfies our requirements. □

Corollary 1.13. *For every at most countable family $\{\phi_i \in \mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \mid i \in \mathbb{N}\}$ of pair-wise distinct endomorphisms, the set of points in $R[\![\boldsymbol{t}]\!]$ whose images through the endomorphisms of the family are pair-wise distinct is a dense subset of $R[\![\boldsymbol{t}]\!]$.*

Proof. Let A be an open subset of $R[\![\boldsymbol{t}]\!]$. Then it contains a set of the form $f + \mathfrak{m}^i$, for some f in A and some positive integer i, that is an open set when R is discrete. Since all automorphisms in $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ are continuous independently by the topology of R, we may apply the previous proposition assuming R discrete and we find a chain of open subsets

$$A \supseteq O_1 \supseteq O_2 \supseteq O_3 \supseteq \dots$$

such that $\phi_j(O_i) \cap \phi_k(O_i) = \emptyset$ for every $i \in \mathbb{N}$ and every $1 \leq j < k \leq i$. Possibly restricting the open subsets at each step, we may also assume that each O_j is of the form $f_j + \mathfrak{m}^{i_j}$ where f_j is in $R[\![\boldsymbol{t}]\!]$ for every $j \in \mathbb{N}$ and $(i_j)_{j\in\mathbb{N}}$ is an increasing sequence of positive integers. Then f_j is a Cauchy sequence and, since $R[\![\boldsymbol{t}]\!]$ is complete [7, Chapter IV, §4], converges to f, the unique element of $\bigcap_{j\in\mathbb{N}}(f_j + \mathfrak{m}^{i_j})$. □

1.3 Automorphisms

Let $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ denote the group of algebra automorphisms of $R[\![\boldsymbol{t}]\!]$ in $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$, that is, automorphisms preserving $\mathfrak{m}$. For every $i \in \mathbb{N}$, the image of ϕ in $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ through the map $\tilde{\chi}_i$ as defined in (1.3) is invertible — the inverse being $\tilde{\chi}_i(\phi^{-1})$ — thus we may consider the map $\chi_i : \mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \to \mathrm{Aut}_R(R[\![\boldsymbol{t}]\!]/\mathfrak{m}^{i+1})$ given by the restriction of $\tilde{\chi}_i$.

Notation 8. For every $i \in \mathbb{N}_0$, we use $\mathrm{Aut}^i_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ to denote the kernel of the homomorphism χ_i.

Of course $\mathrm{Aut}^0_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] = \mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$, as $\mathrm{Aut}_R\left(R[\![\boldsymbol{t}]\!]/\mathfrak{m}\right) \cong \mathrm{Aut}_R R = 1$. So, let us focus on $\mathrm{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$.

Definition. The generalized Nottingham group over R of rank n is defined to be the kernel of χ_1, i. e. $\mathrm{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$.

Every element a of $R[\![\boldsymbol{t}]\!]/\mathfrak{m}^2$ can be uniquely written as $a_0 + \sum_{i=1}^n a_i t_i + \mathfrak{m}^2$ where each a_i is in R. Let ϕ be an R-automorphism of $R[\![\boldsymbol{t}]\!]/\mathfrak{m}^2$ preserving $\mathfrak{m}/\mathfrak{m}^2$. Then ϕ maps a to $a_0 + \sum_{i=1}^n a_i \phi(t_i) + \mathfrak{m}^2$, thus it is uniquely determined by its action on $\mathfrak{m}/\mathfrak{m}^2$ that is isomorphic as an R-module to R^n. Moreover the algebra product on $\mathfrak{m}/\mathfrak{m}^2$ is trivial, that is there are no restrictions on the action of ϕ, except for being an isomorphism of R-module. In other words $\mathrm{Aut}_R\left(R[\![\boldsymbol{t}]\!]/\mathfrak{m}^2\right)$ is isomorphic to $\mathrm{GL}_n(R)$ and therefore we have the following sequence

$$1 \to \mathrm{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \to \mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \to \mathrm{GL}_n(R) \to 1 \tag{1.5}$$

that is exact in $\mathrm{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$.

On the other hand, for every $A = (a_{i,j})_{i,j=1}^n \in \mathrm{GL}_n(R)$, let ϕ_A denote the endomrphism of $R[\![\boldsymbol{t}]\!]$ that maps each t_i to $\sum_{j=0}^n a_{i,j} t_j$. Then, for every $A, B \in \mathrm{GL}_n$, few computations show that the composition of associated endomorphisms ϕ_A and ϕ_B acts on each t_i as ϕ_{AB} does. Thus the function mapping A to ϕ_A is indeed a group morphism from $\mathrm{GL}_n(R)$ to $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$. In other words we are able to exhibit a section for χ_1, so that (1.5) is actually a split extension. Thus, we have proved the following proposition.

Proposition 1.14. *The group* $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ *is isomorphic to* $\mathrm{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \rtimes \mathrm{GL}_n(R)$.

1.4 Group of formal power series n-tuples under substitution

We have already mentioned (Proposition 1.6) that $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is anti-isomorphic to $\mathcal{M}_n(R)$ and we may wonder which elements are invertible in $\mathcal{M}_n(R)$, i. e. what is the image of $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ into $\mathcal{M}_n(R)$.

We start observing that if ϕ is in $\mathrm{Aut}^i_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ for some $i \in \mathbb{N}$, then $\phi(t_j)$ must be equal — for every $j \in \{1, \ldots, n\}$ — to $t_j + f_j$ for some $f_j \in \mathfrak{m}^{i+1}$. Indeed a result by Bourbaki [7, Chapter IV, §4, Lemma 2] assures us that for every n-tuple $(f_j)_{j=1}^n$ of formal power series in $\mathfrak{m}^2$, the operation of substitution of $(t_j + f_j)_{j=1}^n$ defines an automorphism, that is continuous because of Proposition 1.8. Thus, for every positive integer i, the group $\mathrm{Aut}^i_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is anti-isomorphic to the submonoid

$$\mathcal{G}\ell^i_n(R) := \left\{(t_j + f_j)_{j=1}^n \in \mathcal{M}_n(R) \mid f_j \in \mathcal{M}_n^{i+1}(R)\right\}$$

of $\mathcal{M}_n(R)$.

Using Proposition 1.14, we can now give a picture of invertible n-tuples in $\mathcal{M}_n(R)$:

Proposition 1.15. *The automorphism group* $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ *is anti-isomorphic to the subset*

$$\left\{(a_{ij}t_j + f_i)_{i=1}^n \in (R[\![\boldsymbol{t}]\!])^n \mid (a_{ij})_{i,j=1}^n \in \mathrm{GL}_n(R),\ f_i \in \mathfrak{m}^2\right\} \subseteq \mathcal{M}_n(R)$$

under substitution. We use $\mathcal{G}\ell^0_n(R)$ *or — more often —* $\mathcal{G}\ell_n(R)$ *to denote such a group.*

Proof. By Proposition 1.6 and Proposition 1.14 (and their proofs), any $\boldsymbol{f} \in \mathcal{M}_n(R)$ is invertible if and only if it can be written as a composition $\boldsymbol{g} \circ \boldsymbol{h}$ where $\boldsymbol{g}$ equals $(\sum_{j=1}^n a_{ij}t_j)_{i=1}^n$ for some invertible matrix $A = (a_{ij})_{i,j=1}^n$ and $\boldsymbol{h} = (t_i + h_i)_{i=1}^n$ is in $\mathcal{G}\ell^1_n(R)$. Since

$$\boldsymbol{g} \circ \boldsymbol{h} = (\sum_{j=1}^n a_{ij}(t_j + h_j))_{i=1}^n,$$

any invertible n-tuple is in $\mathcal{G}\ell_n(R)$. Conversely, let $\boldsymbol{f} \in \mathcal{M}_n(R)$ be equal to $(\sum_{j=1}^n a_j t_j + f_i)_{i=1}^n$ where each f_i is in $\mathfrak{m}^2$ and $A = (a_{i,j})_{i,j=1}^n$ is in $\mathrm{GL}_n(R)$. Then $\boldsymbol{a} = (\sum_{j=1}^n a_{ij}t_j)_{i=1}^n$ is an invertible n-tuple in $\mathcal{G}\ell_n(R)$ and $\boldsymbol{a}^{-1}$ equals $(\sum_{j=1}^n \bar{a}_{ij}t_j)$ where $(\bar{a}_{ij})_{i,j=1}^n = A^{-1}$. Thus

$$\boldsymbol{f} \circ \boldsymbol{a}^{-1} = (\sum_{j=1}^n a_{ij}(\sum_{k=1}^n \bar{a}_{jk}t_k) + f_i \circ \boldsymbol{a})_{i=1}^n = (t_i + f_i \circ \boldsymbol{a})_{i=1}^n$$

is in $\mathcal{G}\ell^1_n(R)$, and therefore $\boldsymbol{f} = (\boldsymbol{f} \circ \boldsymbol{a}^{-1}) \circ \boldsymbol{a}$ is invertible. □

Corollary 1.16. *Let $\boldsymbol{f} = (f_j)_{j=1}^n$ be in the monoid $\mathcal{M}_n(R)$. Then $\boldsymbol{f}$ is invertible (i. e. it is in $\mathcal{G}\ell_n(R)$) if and only if the Jacobian matrix of $\boldsymbol{f}$*

$$\operatorname{Jac}(\boldsymbol{f}) := \left(\frac{\partial}{\partial t_i} f_j\right)_{i,j=1}^n$$

— where $\frac{\partial}{\partial_i}$ denotes the formal partial derivative with respect to t_i — is an invertible matrix in the monoid of $n \times n$ matrices with coefficients in $R[\![\boldsymbol{t}]\!]$.

Proof. Let f_i be equal to $\sum_{\boldsymbol{\alpha}} f_{i,\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}}$ for every $i \in \{1, \ldots, n\}$. Then $\operatorname{Jac}(\boldsymbol{f}) \equiv (f_{i,\boldsymbol{\epsilon}_j})_{i,j=1}^n$ modulo $\mathfrak{m}$, thus $\det \operatorname{Jac}(\boldsymbol{f}) \equiv \det(f_{i,\boldsymbol{\epsilon}_j})_{i,j=1}^n$ modulo $\mathfrak{m}$ and therefore — since an element of $R[\![\boldsymbol{t}]\!]$ is invertible if and only if the constant term is invertible [7, Chapter IV, §4, Proposition 6] — the Jacobian matrix is invertible if and only if so it is $(f_{i,\boldsymbol{\epsilon}_j})_{i,j=1}^n$, that is, by Proposition 1.15, the n-tuple $\boldsymbol{f}$ is in $\mathcal{G}\ell_n(R)$. □

Notation 9. Some ambiguity may occur in notation when dealing with $\mathcal{M}_n(R)$. This depends on the structure we are putting on it; indeed we are using the same symbol to denote the ideal of $(R[\![\boldsymbol{t}]\!])^n$ — and, as such, subject to ring operations — and the monoid under the operation of substitution, that have the same underlying set. Time by time, the nature of $\mathcal{M}_n(R)$ (and subsets) we are considering should be clear from the context. So, for example, let $\boldsymbol{f}$ and $\boldsymbol{g}$ be n-tuples in $(R[\![\boldsymbol{t}]\!])^n$ and let i be a positive integer. Then, when we say that $\boldsymbol{f} \equiv \boldsymbol{g}$ modulo $\mathcal{M}_n^i(R)$, we are considering $\mathcal{M}_n^i(R)$ as an ideal of $(R[\![\boldsymbol{t}]\!])^n$, therefore it means there exists $\boldsymbol{r} \in \mathcal{M}_n^i(R)$ such that $\boldsymbol{f} = \boldsymbol{g} + \boldsymbol{r}$.

Notation 10. Let $\boldsymbol{f} = (f_i)_{i=1}^n$ be in $(R[\![\boldsymbol{t}]\!])^n$. Then for every $\boldsymbol{\alpha} \in \mathbb{N}_0{}^n$ we write $\boldsymbol{f}^{\boldsymbol{\alpha}}$ for $\prod_{i=1}^n f_i^{\alpha_i}$, whereas $\boldsymbol{f}^j$ stands for $(f_i^j)_{i=1}^n \in (R[\![\boldsymbol{t}]\!])^n$ whenever j is a non-negative integer. With this notational conventions we have

$$(\boldsymbol{f}^{\boldsymbol{\alpha}})^j = \boldsymbol{f}^{j\boldsymbol{\alpha}} = (\boldsymbol{f}^j)^{\boldsymbol{\alpha}},$$

where by $j\boldsymbol{\alpha}$ of course we mean the sum of $\boldsymbol{\alpha}$ with itself j times. Moreover this notation allows us to use $\boldsymbol{t}$ also for the element $(t_i)_{i=1}^n \in (R[\![\boldsymbol{t}]\!])^n$ — that is the identity of $\mathcal{M}_n(R)$ — coherently with the notation introduced in Subsection 1.1.1.

Notation 11. The ring $(R[\![\boldsymbol{t}]\!])^n$ has an obvious structure of free n-ranked $R[\![\boldsymbol{t}]\!]$-module. We use $\boldsymbol{E}_1, \ldots, \boldsymbol{E}_n$ to denote the canonical basis, that is $\boldsymbol{E}_i = (\delta_{i,j})_{j=1}^n \in (R[\![\boldsymbol{t}]\!])^n$ for every $i \in \{1, \ldots, n\}$, where δ_{ij} is the Kronecker delta function on $\{1, \ldots, n\}$ to $R[\![\boldsymbol{t}]\!]$.

Let us summarize the situation of anti-isomorphisms and inclusions through the following diagram. On the left the endomorphism setting is displayed, while on the right there are the n-tuples sets.

$$\begin{tikzcd}
\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] & \cong_{\text{anti}} & \mathcal{M}_n(R) \\
\operatorname{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \arrow[u, hook] & \cong_{\text{anti}} & \mathcal{G}\ell_n(R) \arrow[u, hook] \\
\operatorname{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \arrow[u, hook] & \cong_{\text{anti}} & \mathcal{G}\ell^1_n(R) \arrow[u, hook] \\
\operatorname{Aut}^i_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \arrow[u, hook] & \cong_{\text{anti}} & \mathcal{G}\ell^i_n(R) \arrow[u, hook]
\end{tikzcd}$$

1.4.1 Basic computations

Definition. Let $\boldsymbol{f}$ be an element of $\mathcal{G}\ell_n(R)$. Then if $\boldsymbol{f}$ is not the identity of the group, its depth is defined to be

$$\omega(\boldsymbol{f}) := \max\{i \mid \boldsymbol{f} \in \mathcal{G}\ell^i_n(R)\} \cup \{0\},$$

otherwise it is canonically set to infinity.

As the definition might suggest, the concept of depth is strictly related to the one of order. Indeed, if we extend the definition of order to $(R[\![\boldsymbol{t}]\!])^n$, so that the order of any element $\boldsymbol{f} = (f_i)_{i=1}^n$ in $(R[\![\boldsymbol{t}]\!])^n$ is $\min\{\operatorname{ord}(f_i) \mid 1 \leq i \leq n\}$, we can easily observe that for every $\boldsymbol{t} + \boldsymbol{f}$ in $\mathcal{G}\ell^1_n(R)$, we have $\operatorname{ord}(\boldsymbol{f}) = \omega(\boldsymbol{t} + \boldsymbol{f}) + 1$.

Notation 12. It may happen we need to do some combinatorial computation with elements in ${\mathbb{N}_0}^n$. In order to shorten the length of formulae, we agree on the following conventions: let $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^n$ and $\boldsymbol{\beta} = (\beta_i)_{i=1}^n$ be n-tuples in ${\mathbb{N}_0}^n$, then

$$\boldsymbol{\alpha}! = \prod_{i=1}^n \alpha_i! \qquad \text{and}$$

$$\binom{\boldsymbol{\alpha}}{\boldsymbol{\beta}} = \frac{\boldsymbol{\alpha}!}{\boldsymbol{\beta}!(\boldsymbol{\alpha}-\boldsymbol{\beta})!} = \prod_{i=1}^n \binom{\alpha_i}{\beta_i} \qquad \text{whenever } \boldsymbol{\alpha} \geq \boldsymbol{\beta}, \text{ otherwise } \binom{\boldsymbol{\alpha}}{\boldsymbol{\beta}} = 0.$$

Moreover we will make use of the R-linear operation $\partial_{\boldsymbol{\beta}}$ defined for every $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$ by

$$\partial_{\boldsymbol{\beta}} \boldsymbol{t}^{\boldsymbol{\alpha}} = \binom{\boldsymbol{\alpha}}{\boldsymbol{\beta}} \boldsymbol{t}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} \quad \text{for every } \boldsymbol{\alpha} \in {\mathbb{N}_0}^n. \tag{1.6}$$

Note that when $\boldsymbol{\beta}$ is a generator $\boldsymbol{\epsilon}_j$ of ${\mathbb{N}_0}^n$, then $\partial_{\boldsymbol{\epsilon}_j}$ exactly coincides with the usual formal partial derivative with respect to t_j, whence the choice of notation.

Lemma 1.17. *Let $\boldsymbol{f}$ and $\boldsymbol{g}$ be in $\mathcal{M}_n(R)$. Then*

$$h \circ (\boldsymbol{f} + \boldsymbol{g}) = \sum_{\boldsymbol{\beta} \in {\mathbb{N}_0}^n} \boldsymbol{f}^{\boldsymbol{\beta}} \left((\partial_{\boldsymbol{\beta}} h) \circ \boldsymbol{g}\right)$$

for every $h \in R[\![\boldsymbol{t}]\!]$.

Proof. Let $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^n$ be any n-tuple in ${\mathbb{N}_0}^n$. Then

$$\begin{aligned}
\boldsymbol{t}^{\boldsymbol{\alpha}} \circ (\boldsymbol{f} + \boldsymbol{g}) &= \prod_{i=1}^{n} (f_i + g_i)^{\alpha_i} = \prod_{i=1}^{n} \sum_{0 \le \beta_i \le \alpha_i} \binom{\alpha_i}{\beta_i} {f_i}^{\beta_i} {g_i}^{\alpha_i - \beta_i} = \\
&= \sum_{0 \le \beta_1 \le \alpha_i} \cdots \sum_{0 \le \beta_n \le \alpha_n} \binom{\alpha_1}{\beta_1} {f_1}^{\beta_1} {g_1}^{\alpha_1 - \beta_1} \cdots \binom{\alpha_n}{\beta_n} {f_n}^{\beta_n} {g_n}^{\alpha_n - \beta_n} \\
&= \sum_{\boldsymbol{\beta} \le \boldsymbol{\alpha}} \binom{\boldsymbol{\alpha}}{\boldsymbol{\beta}} \boldsymbol{f}^{\boldsymbol{\beta}} \boldsymbol{g}^{\boldsymbol{\alpha} - \boldsymbol{\beta}} = \sum_{\boldsymbol{\beta} \le \boldsymbol{\alpha}} \boldsymbol{f}^{\boldsymbol{\beta}} \binom{\boldsymbol{\alpha}}{\boldsymbol{\beta}} \boldsymbol{g}^{\boldsymbol{\alpha} - \boldsymbol{\beta}} = \sum_{\boldsymbol{\beta} \le \boldsymbol{\alpha} \le \boldsymbol{\alpha}} \boldsymbol{f}^{\boldsymbol{\beta}} \left(\binom{\boldsymbol{\alpha}}{\boldsymbol{\beta}} \boldsymbol{t}^{\boldsymbol{\alpha} - \boldsymbol{\beta}} \circ \boldsymbol{g} \right) \\
&= \sum_{\boldsymbol{\beta} \le \boldsymbol{\alpha}} \boldsymbol{f}^{\boldsymbol{\beta}} \left((\partial_{\boldsymbol{\beta}} \boldsymbol{t}^{\boldsymbol{\alpha}}) \circ \boldsymbol{g} \right)
\end{aligned}$$

where — since $\partial_{\boldsymbol{\beta}} \boldsymbol{t}^{\boldsymbol{\alpha}} = 0$ whenever $\boldsymbol{\beta} \not\le \boldsymbol{\alpha}$ — we can actually make $\boldsymbol{\beta}$ range all over ${\mathbb{N}_0}^n$. So, let $h \in R[\![\boldsymbol{t}]\!]$ be $h = \sum_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} h_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}}$. Then

$$h \circ (\boldsymbol{f} + \boldsymbol{g}) = \sum_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} h_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}} \circ (\boldsymbol{f} + \boldsymbol{g}) = \sum_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} h_{\boldsymbol{\alpha}} \sum_{\boldsymbol{\beta} \in {\mathbb{N}_0}^n} \boldsymbol{f}^{\boldsymbol{\beta}} \left((\partial_{\boldsymbol{\beta}} \boldsymbol{t}^{\boldsymbol{\alpha}}) \circ \boldsymbol{g} \right).$$

Since $R[\![\boldsymbol{t}]\!]$ is the inverse limit of $\{R[\![\boldsymbol{t}]\!]/\mathcal{M}_n^i(R) \mid i \in \mathbb{N}\}$, both sums $\sum_{\boldsymbol{\beta}}$ and $\sum_{\boldsymbol{\alpha}}$ are the inverse limit of finite sums and can be switched. Moreover, substitution and $\partial_{\boldsymbol{\beta}}$ are R-linear, so

$$h \circ (\boldsymbol{f} + \boldsymbol{g}) = \sum_{\boldsymbol{\beta} \in {\mathbb{N}_0}^n} \boldsymbol{f}^{\boldsymbol{\beta}} \left(\left(\partial_{\boldsymbol{\beta}} \sum_{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n} h_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}} \right) \circ \boldsymbol{g} \right) = \sum_{\boldsymbol{\beta} \in {\mathbb{N}_0}^n} \boldsymbol{f}^{\boldsymbol{\beta}} \left((\partial_{\boldsymbol{\beta}} h) \circ \boldsymbol{g} \right)$$

concludes the proof. □

Proposition 1.18. *Let $\boldsymbol{f} = (t_i + f_i)_{i=1}^n$ and $\boldsymbol{g} = (t_i + g_i)_{i=1}^n$ be in $\mathcal{M}_n(R)$. Then*

$$\boldsymbol{f} \circ \boldsymbol{g} = \boldsymbol{t} + \boldsymbol{g}' + \boldsymbol{f}' + \sum_{\boldsymbol{\alpha} > \boldsymbol{0}} (\boldsymbol{g}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \boldsymbol{f}' \tag{1.7}$$

where $\boldsymbol{f}' = (f_i)_{i=1}^n$ and $\boldsymbol{g}' = (g_i)_{i=1}^n$.

Proof. By Lemma 1.17, we have

$$(t_i + f_i) \circ \boldsymbol{g} = t_i + g_i + \sum_{\boldsymbol{\beta}} (\boldsymbol{g}')^{\boldsymbol{\beta}} \left((\partial_{\boldsymbol{\beta}}(f_i)) \circ \boldsymbol{t} \right) = t_i + g_i + \sum_{\boldsymbol{\beta}} (\boldsymbol{g}')^{\boldsymbol{\beta}} \partial_{\boldsymbol{\beta}}(f_i),$$

thus $\boldsymbol{f} \circ \boldsymbol{g} = \boldsymbol{g} + \sum_{\boldsymbol{\beta}} (\boldsymbol{g}')^{\boldsymbol{\beta}} \partial_{\boldsymbol{\beta}} \left(\boldsymbol{f}' \right)$ whence the claim follows, as $(\boldsymbol{g}')^{\boldsymbol{0}} \partial_{\boldsymbol{0}} \boldsymbol{f}' = \boldsymbol{f}'$. □

By Lemma 1.3 we deduce that the order of $(\boldsymbol{g}')^{\boldsymbol{\beta}} \partial_{\boldsymbol{\beta}} \boldsymbol{f}'$ is at least

$$\operatorname{ord}\left((\boldsymbol{g}')^{\boldsymbol{\beta}} \right) + \operatorname{ord}\left(\partial_{\boldsymbol{\beta}} \boldsymbol{f}' \right) \ge |\boldsymbol{\beta}| \operatorname{ord}\left(\boldsymbol{g}' \right) + \operatorname{ord}\left(\boldsymbol{f}' \right) - |\boldsymbol{\beta}| \ge |\boldsymbol{\beta}| \, \omega\left(\boldsymbol{g} \right) + \omega\left(\boldsymbol{f} \right) + 1;$$

therefore $\omega\left(\boldsymbol{f} \circ \boldsymbol{g} \right) \ge \min\{\omega\left(\boldsymbol{f} \right), \omega\left(\boldsymbol{g} \right)\}$ and we can rewrite (1.7) as

$$\boldsymbol{f} \circ \boldsymbol{g} \equiv \boldsymbol{t} + \boldsymbol{f}' + \boldsymbol{g}' \mod \mathcal{M}_n^{\omega(\boldsymbol{g}) + \omega(\boldsymbol{f}) + 1}(R). \tag{1.8}$$

Corollary 1.19. *For every $j, k \in \mathbb{N}$, the subgroup $\left[\mathcal{G}\ell_n^j(R), \mathcal{G}\ell_n^k(R) \right]$ is contained in $\mathcal{G}\ell_n^{j+k}(R)$.*

Corollary 1.20. *For every $j \in \mathbb{N}$ and every $k \in \mathbb{N}$ such that $j \leq k \leq 2j$, the quotient group $\mathcal{G}\ell_n^j(R)/\mathcal{G}\ell_n^k(R)$ is isomorphic to the additive group $\mathcal{M}_n^{j+1}(R)/\mathcal{M}_n^{k+1}(R)$.*

Proof. Consider the map from $\mathcal{G}\ell_n^j(R)$ to $\mathcal{M}_n^{j+1}(R)/\mathcal{M}_n^{k+1}(R)$ sending each $\boldsymbol{f} = (t_i + f_i)_{i=1}^n$ to $(f_i + \mathfrak{m}^{k+1})_{i=1}^n$. By (1.8) such a map is a group homomorphism whose kernel is $\mathcal{G}\ell_n^k(R)$. □

Corollary 1.21. *Let $\boldsymbol{t}+\boldsymbol{f}$ be in $\mathcal{G}\ell_n^1(R)$ and let k be a positive integer. Then the k-th power $\boldsymbol{t}+\boldsymbol{g}$ of $\boldsymbol{t}+\boldsymbol{f}$ equals*

$$\boldsymbol{t} + k\boldsymbol{f} + \sum_{s=2}^{k}\binom{k}{s}\sum_{\boldsymbol{\alpha}_{s-1},\ldots\boldsymbol{\alpha}_1>\boldsymbol{0}} \boldsymbol{f}^{\boldsymbol{\alpha}_{s-1}}\partial_{\boldsymbol{\alpha}_{s-1}}\left(\boldsymbol{f}^{\boldsymbol{\alpha}_{s-2}}\partial_{\boldsymbol{\alpha}_{s-2}}\left(\ldots\partial_{\boldsymbol{\alpha}_1}\boldsymbol{f}\ldots\right)\right). \tag{1.9}$$

Proof. Let $\boldsymbol{f}_1$ be $\boldsymbol{f}$ and recursively define $\boldsymbol{f}_{s+1}$ to be $\sum_{\boldsymbol{\alpha}_s>\boldsymbol{0}}\boldsymbol{f}^{\boldsymbol{\alpha}_s}\partial_{\boldsymbol{\alpha}_s}\boldsymbol{f}_s$ for any $s \in \mathbb{N}$, so that the claim becomes $\boldsymbol{g} = \sum_{s=1}^{k}\binom{k}{s}\boldsymbol{f}_s$. We proceed by induction, the base case being trivial. So, assume the statement holds for a positive integer k. Then, by equation (1.7), we have

$$\begin{aligned}(\boldsymbol{t}+\boldsymbol{g})\circ(\boldsymbol{t}+\boldsymbol{f}) =& \boldsymbol{t}+\boldsymbol{f}+\boldsymbol{g}+\sum_{\boldsymbol{\alpha}_k>\boldsymbol{0}}\boldsymbol{f}^{\boldsymbol{\alpha}_k}\partial_{\boldsymbol{\alpha}_k}\boldsymbol{g} = \boldsymbol{t}+\boldsymbol{f}+\sum_{s=1}^{k}\binom{k}{s}\boldsymbol{f}_s+\sum_{\boldsymbol{\alpha}_k>\boldsymbol{0}}\boldsymbol{f}^{\boldsymbol{\alpha}_k}\partial_{\boldsymbol{\alpha}_k}\sum_{s=1}^{k}\binom{k}{s}\boldsymbol{f}_s\\ =& \boldsymbol{t}+\sum_{s=1}^{k}\binom{k}{s}\boldsymbol{f}_s+\sum_{s=0}^{k}\binom{k}{s}\boldsymbol{f}_{s+1} = \boldsymbol{t}+\sum_{s=1}^{k}\left(\binom{k}{s}+\binom{k}{s-1}\right)\boldsymbol{f}_s+\boldsymbol{f}_{k+1}\end{aligned}$$

whence the claim follows, since $\binom{k}{s-1}+\binom{k}{s}=\binom{k+1}{s}$. □

Corollary 1.22. *Suppose R is an algebra over a field of positive characteristic p. Then, for every $i \in \mathbb{N}$, the subgroup of $\mathcal{G}\ell_n^1(R)$ generated by p-powers of elements in $\mathcal{G}\ell_n^i(R)$ is contained in $\mathcal{G}\ell_n^{ip}(R)$.*

Let $\boldsymbol{f}=\boldsymbol{t}+\boldsymbol{f}'$ and $\boldsymbol{g}=\boldsymbol{t}+\boldsymbol{g}'$ be elements in $\mathcal{G}\ell_n(R)$. Let $\boldsymbol{h}=\boldsymbol{t}+\boldsymbol{h}'$ be their commutator $[\boldsymbol{f},\boldsymbol{g}]$, that is $\boldsymbol{h}=\boldsymbol{f}^{-1}\circ\boldsymbol{g}^{-1}\circ\boldsymbol{f}\circ\boldsymbol{g}$. Then $\boldsymbol{f}\circ\boldsymbol{g}$ equals $\boldsymbol{g}\circ\boldsymbol{f}\circ\boldsymbol{h}$ and therefore, by (1.7),

$$\boldsymbol{f}\circ\boldsymbol{g} = \boldsymbol{t}+\boldsymbol{h}'+\boldsymbol{g}\circ\boldsymbol{f}-\boldsymbol{t}+\sum_{\boldsymbol{\alpha}>\boldsymbol{0}}(\boldsymbol{h}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\left(\boldsymbol{g}\circ\boldsymbol{f}-\boldsymbol{t}\right),$$

whence, using again equation (1.7) to compute $\boldsymbol{f}\circ\boldsymbol{g}-\boldsymbol{g}\circ\boldsymbol{f}$, we obtain

$$\boldsymbol{h}' = \boldsymbol{f}\circ\boldsymbol{g}-\boldsymbol{g}\circ\boldsymbol{f}-\sum_{\boldsymbol{\alpha}>\boldsymbol{0}}(\boldsymbol{h}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\left(\boldsymbol{g}\circ\boldsymbol{f}-\boldsymbol{t}\right) \tag{1.10}$$

$$= \sum_{\boldsymbol{\alpha}>\boldsymbol{0}}\left((\boldsymbol{g}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\boldsymbol{f}'-(\boldsymbol{f}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\boldsymbol{g}'-(\boldsymbol{h}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\left(\boldsymbol{g}\circ\boldsymbol{f}-\boldsymbol{t}\right)\right). \tag{1.11}$$

Note that $\sum_{\boldsymbol{\alpha}>\boldsymbol{0}}(\boldsymbol{h}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\left(\boldsymbol{g}\circ\boldsymbol{f}-\boldsymbol{t}\right)$ has order at least $\omega(\boldsymbol{h})+1+\omega(\boldsymbol{g}\circ\boldsymbol{f})$, so

$$[\boldsymbol{f},\boldsymbol{g}] \equiv \boldsymbol{t}+\sum_{\boldsymbol{\alpha}>\boldsymbol{0}}\left((\boldsymbol{g}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\boldsymbol{f}'-(\boldsymbol{f}')^{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}}\boldsymbol{g}'\right) \mod \mathcal{M}_n^{\omega([\boldsymbol{f},\boldsymbol{g}])+\min\{\omega(\boldsymbol{f}),\omega(\boldsymbol{g})\}+1}(R). \tag{1.12}$$

We already stressed the double nature of elements in $\mathcal{M}_n(R)$: they are both endomorphism (acting through $\circ$ on elements of $R[\![\boldsymbol{t}]\!]$ or even on other endomorphisms) and elements of the R-ideal $\mathcal{M}_n(R)$ of $(R[\![\boldsymbol{t}]\!])^n$ (that can be added and multiplied). The following simple lemma will justify and give more solidity to our fluid approach in passing from one view to the other without too much worrying.

Lemma 1.23. *Let $\boldsymbol{f}$ and $\boldsymbol{g}$ be in $\mathcal{G}\ell_n(R)$. Then $\boldsymbol{f}$ and $\boldsymbol{g}$ are equivalent modulo $\mathcal{M}_n^{i+1}(R)$ (as elements of the ring $(R[\![\boldsymbol{t}]\!])^n$) for some $i \in \mathbb{N}$ if and only if they are equivalent modulo $\mathcal{G}\ell_n^i(R)$ (as elements of the group $\mathcal{G}\ell_n(R)$).*

Proof. This is essentialy due to the fact that $h \circ \boldsymbol{g}$ is in $\mathfrak{m}^{i+1}$ if so it is h.

Let $\boldsymbol{r}$ be of order greater than i and suppose $\boldsymbol{f}$ is equal to $\boldsymbol{g} + \boldsymbol{r}$. Then $\boldsymbol{f} \circ \boldsymbol{g}^{-1}$ equals $\boldsymbol{g} \circ \boldsymbol{g}^{-1} + \boldsymbol{r} \circ \boldsymbol{g}^{-1}$ where $\boldsymbol{g} \circ \boldsymbol{g}^{-1} = \boldsymbol{t}$ and each component of the n-tuple $\boldsymbol{r} \circ \boldsymbol{g}^{-1}$ is in $\mathfrak{m}^{i+1}$, that is to say $\boldsymbol{f} \circ \boldsymbol{g}^{-1}$ is in $\mathcal{G}\ell_n^i(R)$. Conversely, if $\boldsymbol{f} \circ \boldsymbol{g}^{-1} = \boldsymbol{t} + \boldsymbol{r}$ is in $\mathcal{G}\ell_n^i(R)$, i. e. the order of $\boldsymbol{r}$ is greater than i, then $\boldsymbol{f} = \boldsymbol{g} + \boldsymbol{r} \circ \boldsymbol{g}$ with $\boldsymbol{r} \circ \boldsymbol{g}$ lying in $\mathcal{M}_n^{i+1}(R)$. □

1.5 Topology

So far we have treated the appeared groups of automorphisms as abstract groups. However we saw that $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is anti-isomorphic to $\mathcal{M}_n(R)$ under substitution — and indeed since then we have been mostly working with such a representation —, therefore we may endow it with the natural topology inherited by $(R[\![\boldsymbol{t}]\!])^n$, that is the product topology.

Notation 13. From now on, the monoid $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ and all submonoids — wether seen as a subsets of $(R[\![\boldsymbol{t}]\!])^n$ or not — are meant to be endowed with the just mentioned topology. In particular we are going to prove that the Nottingham group is a topological group.

Lemma 1.24. *Each set of the chain $\mathcal{M}_n(R) \supseteq \mathcal{G}\ell_n^1(R) \supseteq \mathcal{G}\ell_n^2(R) \supseteq \dots$ is closed in $(R[\![\boldsymbol{t}]\!])^n$.*

Proof. Each $\mathcal{M}_n^i(R)$ is closed — by definition of product topology — because it is the direct product of n copies of the closed set $\mathfrak{m}^i$ in $(R[\![\boldsymbol{t}]\!])^n$. This implies that also each $\mathcal{G}\ell_n^i(R)$ — that coincides as a subset of $(R[\![\boldsymbol{t}]\!])^n$ with the coset $\boldsymbol{t} + \mathcal{M}_n^{i+1}(R)$ — is closed. □

Thus, in particular (see Proposition A.6)

Lemma 1.25. *As topological spaces, we have*

$$\begin{aligned} \mathcal{M}_n(R) &= \varprojlim \mathcal{M}_n(R)/\mathcal{M}_n^i(R) \\ \boldsymbol{t} + \mathcal{M}_n^j(R) &= \varprojlim((\boldsymbol{t} + \mathcal{M}_n^j(R))/\mathcal{M}_n^i(R)) \qquad \text{for every } j \in \mathbb{N} \end{aligned}$$

where the maps defining the inverse systems are the restrictions of canonical projections from $(R[\![\boldsymbol{t}]\!])^n/\mathcal{M}_n^{i_1}(R)$ to $(R[\![\boldsymbol{t}]\!])^n/\mathcal{M}_n^{i_2}(R)$, that are well defined whenever $i_1 > i_2$.

Regarding $\mathcal{G}\ell_n(R)$, topology depends also on the topology of R.

Lemma 1.26. *If $R^\times$ is open (resp. closed) in R, then $\mathcal{G}\ell_n(R)$ is open (resp. closed) in $\mathcal{M}_n(R)$.*

Proof. This is simply due to the fact that $\mathcal{G}\ell_n(R)$ is — by Corollary 1.16 — the inverse image of $R^\times$ through the map

$$\mathcal{M}_n(R) \to \mathcal{M}_n(R)/\mathcal{M}_n^2(R) \cong R^{n\times n} \to R$$

that is the composition of the canonical projection with the computation of the determinant when $\mathcal{M}_n(R)/\mathcal{M}_n^2(R)$ is seen as the set of $n \times n$ matrices over R. Both these maps are continuous. □

Lemma 1.27. *The map from $R[\![\boldsymbol{t}]\!] \times \mathcal{M}_n(R)$ to $R[\![\boldsymbol{t}]\!]$ that, for every $f \in R[\![\boldsymbol{t}]\!]$ and for every $\boldsymbol{g} \in \mathcal{M}_n(R)$, sends $(f, \boldsymbol{g})$ to $f \circ \boldsymbol{g}$ is continuous.*

Proof. By Proposition 1.4, it is enough to show that, for every positive integer i, the well defined map from $(R[\![\boldsymbol{t}]\!]/\mathfrak{m}^i) \times \mathcal{M}_n(R)$ to $R[\![\boldsymbol{t}]\!]/\mathfrak{m}^i$ which sends $(f + \mathfrak{m}^i, \boldsymbol{g})$ to $f \circ \boldsymbol{g} + \mathfrak{m}^i$ is continuous. Such a map may be seen as the function from $\left(\prod_{|\boldsymbol{\alpha}| \leq i+1} R\boldsymbol{t}^{\boldsymbol{\alpha}}\right) \times \mathcal{M}_n(R)$ to $R[\![\boldsymbol{t}]\!]/\mathfrak{m}^i$ that sends $\left((r_{\boldsymbol{\alpha}})_{|\boldsymbol{\alpha}| \leq i+1}, \boldsymbol{g}\right)$ to $\sum_{|\boldsymbol{\alpha}| \leq i+1} r_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}} \circ \boldsymbol{g} + \mathfrak{m}^i$, that is a composition of continuous functions, since $R[\![\boldsymbol{t}]\!]$ is a topological ring. □

Corollary 1.28. *For every open subset $O \subseteq R[\![\boldsymbol{t}]\!]$ and every formal power series f in $R[\![\boldsymbol{t}]\!]$, the subset of $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ whose elements are endomorphisms $\phi \in \operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ that map f into O is open. Moreover, subsets of this form generate the topology of $\mathcal{M}_n(R)$.*

Proof. As usual we identify $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ and $\mathcal{M}_n(R)$. Consider the function $\mathfrak{m} \to R[\![\boldsymbol{t}]\!]$ that maps $\boldsymbol{g}$ to $f \circ \boldsymbol{g}$. It is continuous because of the previous lemma, so the preimage of O, that is $\{\boldsymbol{g} \in \mathcal{M}_n(R) \mid f \circ \boldsymbol{g} \in O\}$, is open.

Since $\mathcal{M}_n(R) = \prod_{i=1}^n \mathfrak{m}$ is endowed with the product topology, a base for the topology is given by sets of the form $O_1 \times \ldots \times O_n$, where each O_i is an open subset of $\mathfrak{m}$. Such a set can be obtained as intersection of the sets $\{\boldsymbol{g} \in \mathcal{M}_n(R) \mid t_i \circ \boldsymbol{g} \in O_i\}$ for $i \in \{1, \ldots, n\}$, whence the second part of the statement follows. □

Lemma 1.29. *The map from $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \times \operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ to $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ given by composition of endomorphisms is continuous.*

Proof. As usual, we identify $\operatorname{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ with $\mathcal{M}_n(R)$, so that the interested map may be written as

$$\boldsymbol{f} \circ \boldsymbol{g} \mapsto (f_i \circ \boldsymbol{g})_{i=1}^n \qquad \text{for every } \boldsymbol{f} = (f_i)_{i=1}^n, \boldsymbol{g} \in \mathcal{M}_n(R)$$

and, since $\mathcal{M}_n(R)$ has the product topology of $\mathfrak{m}$ with itself n times, it is continuous if and only if each component of the map is continuous. But these are exactly the maps from $\mathfrak{m} \times \mathcal{M}_n(R)$ to $\mathfrak{m}$ sending each pair $(f_i, \boldsymbol{g})$ to $f_i \circ \boldsymbol{g}$ which were proved to be continuous in Lemma 1.27. □

Proposition 1.30. *The generalized Nottingham group is a topological group.*

Proof. By Lemma 1.29, the composition is continuous. Therefore it only remains to check continuity of the inversion map. Let $\boldsymbol{f}^{-1} = \boldsymbol{t} + \boldsymbol{f}^*$ be the inverse of $\boldsymbol{f} = \boldsymbol{t} + \boldsymbol{f}' \in \mathcal{G}\ell_n^1(R)$. By equation (1.7) we deduce

$$\boldsymbol{f}^* = -\boldsymbol{f}' - \sum_{\boldsymbol{\alpha} > \boldsymbol{0}} (\boldsymbol{f}^*)^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \boldsymbol{f}'$$

that modulo $\mathcal{M}_n^{i+1}(R)$, for some $i \in \mathbb{N}$, becomes

$$\boldsymbol{f}^* \equiv \lfloor \boldsymbol{f}^* \rfloor_i \equiv -\lfloor \boldsymbol{f}' \rfloor_i - \sum_{0 < |\boldsymbol{\alpha}| \leq i} (\lfloor \boldsymbol{f}^* \rfloor_{i-1})^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \lfloor \boldsymbol{f}' \rfloor_{i-1} \mod \mathcal{M}_n^{i+1}(R)$$

where — for every $\boldsymbol{g} \in \mathcal{M}_n(R)$ and every $j \in \mathbb{N}$ — by $\lfloor \boldsymbol{g} \rfloor_j$ we mean the lowest-degree representative in $\mathcal{M}_n(R)$ of the equivalence class $\boldsymbol{g} + \mathcal{M}_n^{j+1}(R)$, that we call truncated polynomial $\boldsymbol{g}$ to j. Now we have that for every $i \in \mathbb{N}$ the map $\boldsymbol{f} \mapsto -\lfloor \boldsymbol{f}' \rfloor_i$ is easily seen to be continuous and therefore we obtain by induction that so it is each map $\boldsymbol{f} \mapsto \lfloor \boldsymbol{f}^* \rfloor_{i+1}$, being composition of continuous functions. It follows that also the inversion map is continuous, since it is the inverse limit of the maps sending $\boldsymbol{f}$ to $\boldsymbol{t} + \lfloor \boldsymbol{f}^* \rfloor_i$. □

Corollary 1.31. *The map $\operatorname{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!] \to \operatorname{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ given by inversion is continuous and in particular $\operatorname{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is a topological group.*

Proof. The group of automorphisms is (topologically) isomorphic to $\mathrm{GL}_n(R) \ltimes \mathcal{G}\ell_n^1(R)$, by Proposition 1.14. So the inversion map can be seen as a function from the topological product of $\mathrm{GL}_n(R)$ and $\mathcal{G}\ell_n^1(R)$ to $\mathcal{G}\ell_n(R)$ that maps $(\boldsymbol{a}, \boldsymbol{f})$ to $\boldsymbol{f}^{-1} \circ \boldsymbol{a}^{-1}$, where $\boldsymbol{f}$ is in $\mathcal{G}\ell_n^1(R)$ and $\boldsymbol{a} \in \mathcal{M}_n(R)$ is the n-tuple $(\sum_{j=1}^n a_{ij}t_j)_{i=1}^n$ associated to an invertible matrix $A = (a_{ij})_{i,j=1}^n$ in $\mathrm{GL}_n(R)$. Inversion in $\mathrm{GL}_n(R)$ and — by the previous lemma — inversion in $\mathcal{G}\ell_n^1(R)$ are continuous. Since composition is also continuous, we obtain the desired result. □

Each $\mathcal{G}\ell_n^i(R)$ is a closed normal subgroup of $\mathcal{G}\ell_n(R)$. By Lemma 1.23, the projection from $\mathcal{G}\ell_n(R)$ to $\mathcal{G}\ell_n(R)/\mathcal{G}\ell_n^i(R)$ coincides with the restriction to $\mathcal{G}\ell_n(R)$ of the projection from $\mathcal{M}_n(R)$ onto $\mathcal{M}_n(R)/\mathcal{M}_n^{i+1}(R)$, whence we deduce that the inverse limit defined in Lemma 1.25 is indeed an inverse limit of groups, even topological groups by previous results.

Remark 1.32. When R is discrete, proving that $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is a topological group is much easier. Indeed, in such a case, the normal subgroups $\{\mathcal{G}\ell_n^i(R) \mid i \in \mathbb{N}\}$ form a base for the neighbourhoods of the identity and the result follows from Proposition C.1.

Proposition 1.33. *Let R be a finite ring. Then $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is a profinite group. Furthermore, if $(R, +)$ is a p-group for some prime p, then $\mathcal{G}\ell_n^1(R)$ is a pro-p group.*

Proof. Since R is discrete, each $\mathcal{G}\ell_n^i(R)$ is open and closed for every non-negative integer i. Since R is finite, the group $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is a closed subset of the compact $(R[\![\boldsymbol{t}]\!])^n$. Thus $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ is Hausdorff, compact and has a base for the open neighbourhoods of the identity given by open normal subgroups $\{\mathcal{G}\ell_n^i(R) \mid i \in \mathbb{N}\}$.

By Corollary 1.20, if $(R, +)$ is a p-group, then each quotient $\mathcal{G}\ell_n^i(R)/\mathcal{G}\ell_n^i(R)$ is a p-group for every $i \in \mathbb{N}$ and therefore $\mathcal{G}\ell_n^1(R)$ is pro-p. □

Chapter 2

The associated Lie algebra

In this chapter we adapt to our case an argument often used for pro-p groups. Most of definitions and result given in this introduction can be found in [34].

When G is a profinite group, a filtration of G is usually defined to be a chain of open normal subgroups

$$G = G_1 \geq G_2 \geq G_3 \geq \dots$$

such that $\bigcap G_i = 1$. A filtration $\{G_i\}$ of G is called an N-series if the subgroup $[G_i, G_j]$ is contained in G_{i+j} for every $i, j \in \mathbb{N}$.

When G is pro-p for some prime p, an N_p-series is an N-series $\{G_i\}$ such that $G_i^p \subseteq G_{pi}$, where $G_i^p = \langle g^p \mid g \in G_i \rangle$.

So assume we have a pro-p group G with an open N-series $\{G_i\}$. Then each quotient G_i/G_{i+1} is an abelian finite group, so that we can construct an additive abelian group $L(G) := \bigoplus_{i \in \mathbb{N}} G_i/G_{i+1}$, where the group operation is denoted by $+$ and each element in $L(G)$ is written in formal series form as $\sum_{i \in \mathbb{N}} x_i$ where each x_i is in G_i/G_{i+1} and it is trivial for all but finitely many $i \in \mathbb{N}$. Moreover there is a well defined function from the direct product of G_i/G_{i+1} and G_j/G_{j+1} to G_{i+j}/G_{i+j+1} that maps (xG_{i+1}, yG_{j+1}) to $[x, y]\, G_{j+i+1}$. This allows us to define a Lie ring structure on $L(G)$, imposing additivity on each component to this latter operation. When $\{G_i\}$ is also an N_p-series, then each factor is an elementary abelian p-group — i. e. isomorphic to a vector space over the finite field of order p — and therefore we can even consider $L(G)$ as a Lie algebra over this finite field, where product by a scalar is given by an integer power in the group. Indeed we might define also a p-exponentiation operation which makes it turn into a restricted Lie algebra [34], however, since we are not going to use it we do not care about it.

In this chapter we are essentially going to construct and study the Lie ring associated in similar manner to $\mathcal{G}\ell_n^1(R)$ (that might not be a profinite group, if R is not a profinite ring). As it turns out that such a Lie ring is strictly related to the algebra of derivations of $R[\![\boldsymbol{t}]\!]$, we start studying the latter one.

2.1 The derivation algebra of the formal power series ring

Here we introduce the derivation algebra of $R[\![\boldsymbol{t}]\!]$. There is nothing essentially new, but it is rather some folklore results organized for our purpose.

Definition. Let A be an R-algebra. A derivation of A is an R-linear endomorphism $D : A \to A$ such that $D(ab) = aD(b) + D(a)b$ for every $a, b \in A$.

Let $\operatorname{Der}_R(A)$ denote the set of derivations and let us focus on $A = R[\![\boldsymbol{t}]\!]$. The simplest example of derivation is the usual formal partial derivative with respect to any $i \in \{1, \dots, n\}$, that is the linear map $\partial_i := \frac{\partial}{\partial t_i}$ such that $\partial_i \boldsymbol{t}^{\boldsymbol{\alpha}} = \alpha_i \boldsymbol{t}^{\boldsymbol{\alpha}-\boldsymbol{\epsilon}_i}$ for every $\boldsymbol{\alpha} = (\alpha_j)_{j=1}^n$. Indeed, as the following lemma shows, all derivations are built from formal partial derivatives.

Lemma 2.1. *The set* $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ *is a free* $R[\![\boldsymbol{t}]\!]$*-module, a basis of which is given by the set of formal partial derivatives.*

Proof. It is a well known general fact that $\operatorname{Der}_R(A)$ is an A-module, so we only prove that the formal partial derivatives form a base.

First of all we note that every derivation D is uniquely determined by the images of all monomials t_i, since, for any formal power series $f = \sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}}$ in $R[\![\boldsymbol{t}]\!]$, the image of f through D equals $\sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}} D(\boldsymbol{t}^{\boldsymbol{\alpha}})$. In turn, for every $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^n \in {\mathbb{N}_0}^n$,

$$D(\boldsymbol{t}^{\boldsymbol{\alpha}}) = \sum_{i=1}^{n} D(t_i^{\alpha_i}) \prod_{j \neq i} t_j^{\alpha_j}$$

where $D(t_i^{\alpha_i}) = \sum_{j=1}^{\alpha_i} D(t_i) t_i^{\alpha_i - 1}$. So, the linear endomorphism $\sum_{i=1}^n D(t_i)\partial_i$ acts exactly like D on the arbitrarily chosen f and thus it is indeed D itself. This proves that $\{\partial_i \mid i \in \{1, \dots, n\}\}$ generates $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$.

Suppose that $\sum_{i=1}^n a_i \partial_i = 0$ for some n-tuple $(a_i)_{i=1}^n \in (R[\![\boldsymbol{t}]\!])^n$. Then $0 = \sum_{i=1}^n a_i \partial_i(t_j) = a_j$ for every $j \in \{1, \dots, n\}$. Therefore the formal partial derivatives are linearly independent. □

Indeed we can even endow $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ with a further operation. Let D and E be two derivations. Then the composition DE is not in general a derivation. However the function

$$[D, E] := DE - ED : f \mapsto D(E(f)) - E(D(f))$$

maps pairs of derivations to derivations. Thus we have a binary function $[\ ,\ ]$ from $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!]) \times \operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ to $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ that — one might verify — satisfies the axioms for a Lie R-algebra.

For every integer $j \geq -1$ define $\operatorname{Der}_R^j(R[\![\boldsymbol{t}]\!])$ to be the $R[\![\boldsymbol{t}]\!]$-submodule $\bigoplus_{i=1}^n \mathfrak{m}^{j+1}\partial_i$ of $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$. These are indeed Lie subalgebras and later on we are going to see their importance.

Remark 2.2. Indeed $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ is a completed graded Lie algebra, in that

$$\operatorname{Der}_R(R[\![\boldsymbol{t}]\!]) = \prod_{i \geq -1} \hom_i$$

where $\hom_i = \bigoplus_{j=1}^n \left(\bigoplus_{|\boldsymbol{\alpha}|=i+1} R\boldsymbol{t}^{\boldsymbol{\alpha}} \right) \partial_j$ is the set of homogeneous elements of degree $i+1$ and $[\hom_i, \hom_j] \subseteq \hom_{i+j}$ for every $i \geq -1$ and $j > -1$ (whereas $[\hom_{-1}, \hom_{-1}] = 0$).

We conclude this section with a simple lemma that we shall use in Chapter 4.

Lemma 2.3. *Let $\rho : R \to S$ be a ring homomorphism, thus in particular S may be considered as an R-algebra. Then there is a natural morphism of Lie R-algebras* $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!]) \to \operatorname{Der}_S(S[\![\boldsymbol{t}]\!])$ *that preserves gradation. If ρ is injective, then* $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ *embeds into* $\operatorname{Der}_S(S[\![\boldsymbol{t}]\!])$.

Proof. The desired map is given by $\sum_{i=1}^n f_i \partial_i \in \operatorname{Der}_R(R[\![\boldsymbol{t}]\!]) \mapsto \sum_{i=1}^n \rho(f_i)\partial_i \in \operatorname{Der}_S(S[\![\boldsymbol{t}]\!])$. □

2.2 N-series for topological groups and associated Lie rings

We now formalize the idea given in the introduction of this chapter. Let G be an Hausdorff topological group.

Definition. A filtration of G is a chain of closed and normal subgroups $\{G_i \mid i \in \mathbb{N}\}$ (by convention $G_1 = G$) such that $G \cong \varprojlim G/G_i$. A filtration $\{G_i\}$ is called an N-series if $[G_i, G_j] \subseteq G_{i+j}$ for every $i, j \in \mathbb{N}$. When p is a prime, an N-series is called N_p-series if moreover the closed subgroup generated by p-power of elements in G_i is contained in G_{ip} for every $i \in \mathbb{N}$.

Remark 2.4. The definition of N_p-series does not really make much sense except for G being pro-p.

So, let $\{G_i\}$ be an N-series. Then each quotient G_i/G_{i+1} is abelian and we usually use additive notation for it. Moreover, being the quotient over a closed subgroup, it is an Hausdorff topological group.

Let $L(G)$ be the *Cartesian product* of abelian topological groups $\prod_{i\in\mathbb{N}} G_i/G_{i+1}$. It is of course an abelian Hausdorff topological group. An element g of such a group is usually denoted by a formal series $\sum_{i\in\mathbb{N}} g_i G_{i+1}$ where each g_i is in G_i and each $g_i G_{i+1}$ is called homogeneous component of g of degree i. Such a notation is coherent with the additive notation for each quotient, in that — given two elements $\sum_{i\in\mathbb{N}} g_i G_{i+1}$ and $\sum_{i\in\mathbb{N}} h_i G_{i+1}$ — their sum in $L(G)$ is given by $\sum_{i\in\mathbb{N}}(g_i G_{i+1} + h_i G_{i+1}) = \sum_{i\in\mathbb{N}} g_i h_i G_{i+1}$.

Since $\{G_i\}$ is an N-series we can also introduce a brackets operation by imposing

$$[g_i G_{i+1}, h_j G_{j+1}] := [g_i, h_j]\, G_{i+j+1}$$

for every $i, j \in \mathbb{N}$ and every $g_i \in G_i$, $h_j \in G_j$. Then we extend this operation “by linearity”, that is, for all $\sum_{i\in\mathbb{N}} g_i G_{i+1}$ and $\sum_{j\in\mathbb{N}} h_j G_{j+1}$ in $L(G)$,

$$\left[\sum_{i\in\mathbb{N}} g_i G_{i+1}, \sum_{j\in\mathbb{N}} h_j G_{j+1}\right] := \sum_{l\in\mathbb{N}} \sum_{i+j=l} [g_i, h_j]\, G_{l+1} \tag{2.1}$$

where the inner summation of the right-hand side is an actual finite sum in G_l/G_{l+1}, whereas all the others are formal.

One can verify that $[\ ,\ ]$ satisfies — for every $g = \sum_{i\in\mathbb{N}} g_i G_{i+1}$, $h = \sum_{j\in\mathbb{N}} h_j G_{j+1}$ and $f = \sum_{l\in\mathbb{N}} f_l G_{l+1}$ in $L(G)$ — the following properties.

- The brackets operation of g with itself equals $\sum_{l\in\mathbb{N}} 1G_{i+1}$ that is the zero element $0_{L(G)}$ of $L(G)$. This is because $[g_i G_{i+1}, g_j G_{j+1}] + [g_j G_{j+1}, g_i G_{i+1}]$ by definition equals the homogeneous component $[g_i, g_j]\,[g_j, g_i]\, G_{i+j+1} = 1G_{i+j+1}$ while $[g_i G_{i+1}, g_i G_{i+1}]$ equals $[g_i, g_i]\, G_{2i+1}$ that is $1G_{2i+1}$, so that terms in the inner summation in (2.1) cancel.
- The brackets operation of $f + g$ and h equals $[f, h] + [g, h]$. For $[f_i G_{i+1} + g_i G_{i+1}, h_j G_{j+1}]$ equals $[f_i g_i, h_j]\, G_{i+j+1}$ where the commutator $[f_i g_i, h_j]$ is equivalent to $[f_i, h_j]\,[g_i, h_j]$ modulo G_{i+j+1}. Similarly on the right component and therefore $[\ ,\ ]$ is bilinear.
- Jacobi identity: $[[f, g], h] + [[g, h], f] + [[h, f], g] = 0_{L(G)}$ since, by Lemma C.2, we have that $[[f_l, g_i], h_j]\,[[g_i, h_j], f_l]\,[[h_j, f_l], g_i]$ is in $G_{i+j+l+1}$.

So the brackets operation is actually a *Lie* brackets operation and thus we may look at $L(G)$ as a Lie ring. We will see that it is possible to recover results about the group from such a Lie ring. In this perspective, we introduce a natural map $\iota_G : G \to L(G)$ that maps each non-trivial element g of G to $gG_{i(g)} \in L(G)$ — where $i(g)$ is the depth of g with respect to the filtration $\{G_i\}$, namely the maximum among positive integers i such that g is in G_i — and the identity of the group to $0_{L(G)}$.

Notation 14. The structure of $L(G)$ heavily depends on the chosen filtration. However, since most of times it is clear which filtration we are dealing with, our notation safely forgets about it. The same applies to the map ι_G.

Remark 2.5. Note that in chapter's introduction we defined the Lie ring by taking the direct sum of the quotients. Indeed some authors, also for the profinite case, consider the Cartesian product. The reason to prefer the Cartesian product to direct sum is due to the fact that there is a somewhat natural homeomorphism $G \simeq L(G)$. Indeed, let $L_i(G)$ denote the subset $\prod_{j\geq i} G_j/G_{j+1}$ of $L(G)$; then $L_i(G)$ is easily seen to be a closed ideal of $L_i(G)$ and $L(G)$ is homeomorphic to the inverse limit $\varprojlim L(G)/L_i(G)$. The following lemma shows that there exists an homeomorphism of $L(G)/L_i(G)$ and G/G_i compatible with the respective inverse systems, implying the desired homeomorphism of G and $L(G)$ (see also Remark A.2).

Lemma 2.6. *For every positive integer i there exists an homeomorphism f_i from G/G_{i+1} to $P_{i+1} := \bigoplus_{j=1}^{i} G_j/G_{j+1}$.*

Proof. We proceed by induction on i. When $i = 1$ the claim is trivial. For every $gG_i \in G/G_i$ let $\{gG_i\}_i$ denote a representative of the equivalence class gG_i in G/G_{i+1}. Since the canonical map $G/G_{i+1} \to G/G_i$ is continuous and open, its section given by $gG_i \to \{gG_i\}_i$ is continuous. By inductive hypothesis, there exists an homeomorphism $f_i : G/G_i \to P_i$. Then consider the map $f_{i+1} : G/G_{i+1} \to P_{i+1}$ such that $f_{i+1}(gG_{i+1}) = (f_i(gG_i), \{gG_i\}_i^{-1} gG_{i+1})$. It is continuous and bijective, the inverse given by

$$f_{i+1}^{-1}\left((g_jG_{j+1})_{j=1}^{i}\right) = \{f_i^{-1}\left((g_jG_{j+1})_{j=1}^{i-1}\right)\}_i g_i G_{i+1}$$

that is also continuous. □

Proposition 2.7. *Let $\{G_i\}$ be an N-series of a topological group G. Let H be a closed subgroup of G. Then $\{H_i := G_i \cap H\}$ is an N-series for H and the associated Lie ring $L(H)$ of H with respect to such an N-series is isomorphic to the Lie subring $L_G(H)$ of $L(G)$ topologically generated by $\iota_G(H) = \{\iota_G(h) \mid h \in H\}$.*

Moreover, if H is normal, then the associated subalgebra is a Lie ideal.

Proof. It is easy to verify that $\{H_i\}$ is an N-series (see also Proposition A.6). Then $L(H)$ is by definition $\prod_{i\in\mathbb{N}} H_i/H_{i+1}$. Consider the closed additive subgroup $L_G(H)$ of $(L(G), +)$ generated by $\iota_G(H)$, that is $\prod_{i\in\mathbb{N}}(G_i \cap H)G_{i+1}/G_{i+1}$. Then — by isomorphisms theorems — each quotient is isomorphic to $(G_i \cap H)/(G_{i+1} \cap H)$, that is H_i/H_{i+1}, and therefore we have a (continuous) group isomorphism of $L_G(H)$ and $L(H)$. Moreover this isomorphism maps $[hH_{i+1}, fH_{j+1}] = [h, f]\, H_{i+j+1}$ to $[h, f]\, G_{i+j+1} = [hG_{i+1}, fG_{j+1}]$, implying in particular that $L_G(H)$ is closed under Lie brackets and its induced Lie subring structure is isomorphic to $L(H)$.

Finally, if H is normal, for every homogeneous element hG_{i+1} in $L_G(H)$ and every homogeneous element gG_{j+1} in $L(G)$, we may assume h is in H and therefore we have that $[hG_{i+1}, gG_{j+1}]$ equals $[h, g]\, G_{i+j+1}$ that is in $L_G(H)$, since $[h, g]$ is in H. Thus extending to non-homogeneous elements, we have that $[\sum h_iG_{i+1}, \sum g_jG_{j+1}] \in L_G(H)$ for every $\sum h_iG_{i+1} \in L_G(H)$ and every $\sum g_jG_{j+1} \in L(G)$. □

Remark 2.8. A side effect of this last proof is that homogeneous elements of $L_G(H) \subseteq L(G)$ of degree $i \in \mathbb{N}$ are precisely $\{\iota_G(h) = hG_{i+1} \mid h \in (G_i \setminus G_{i+1}) \cap H\}$.

Lemma 2.9. *Let $H_1 \subseteq H_2$ be closed subgroups of G such that the associated Lie subrings $L_G(H_1) = \overline{\langle \iota_G(H_1) \rangle}$ and $L_G(H_2) = \overline{\langle \iota_G(H_2) \rangle}$ of $L(G)$ coincides. Then $H_1 = H_2$.*

Proof. Suppose, by contradiction, there exists h in $H_2 \setminus H_1$, say $h \in G_{i_0} \setminus G_{i_0+1}$. Then there exists $g_1 \in H_1$ such that $\iota_G(g_1) = \iota_G(h)$. Let h_1 be $g_1^{-1}h$. Then h_1 is in $(H_2 \setminus H_1) \cap (G_{i_1} \setminus G_{i_1+1})$, for some $i_1 > i_0$, and there exists $g_2 \in H_1$ such that $\iota_G(h_1) = \iota_G(g_2)$. Iterating, we can construct a sequence $\{g_j \mid j \in \mathbb{N}\} \subseteq H_1$ and an increasing sequence $\{i_j\} \subseteq \mathbb{N}$ such that $g_j \in G_{i_j} \setminus G_{i_j+1}$ and $\left(\prod_{1 \leq k \leq j} g_k\right)^{-1} h \in G_{i_j+1}$. Since every open neighbourhood of the identity must contain some G_i (see Lemma A.5), it follows that h is in the closure of H_1, yielding a contradiction since H_1 is closed. □

Proposition 2.10. *Let H be a closed subgroup of G and let $S \subseteq H$ be such that $\iota_G(S)$ (topologically) generates the subring of $L(G)$ associated to H. Then S (topologically) generates H.*

Proof. Let H_1 be the closed group generated by S. Then $H_1 \leq H$ and therefore $L_G(H) \supseteq L_G(H_1)$. On the other hand $L_G(H_1)$ contains the Lie ring generated by $\iota_G(S)$, that is $L_G(H_1) = L_G(H)$. Thus applying the previous lemma, we obtain that $H_1 = H$. □

2.3 The Lie ring associated to the generalized Nottingham group

We proved in the previous chapter that $\{\mathcal{G}\ell_n^i(R)\}$ is an N-series, in our definition. So we associate to $\mathcal{G}\ell_n^1(R)$ the Lie ring $L(\mathcal{G}\ell_n^1(R))$ and we study it to obtain results about $\mathcal{G}\ell_n^1(R)$ itself.

Let $\boldsymbol{g} = \boldsymbol{t} + \boldsymbol{g}' = (t_l + g_l)_{l=1}^n$ and $\boldsymbol{h} = \boldsymbol{t} + \boldsymbol{h}' = (t_l + h_l)_{l=1}^n$ be in $\mathcal{G}\ell_n^1(R)$. Then, by equation (1.12), we have

$$[\boldsymbol{g}, \boldsymbol{h}] \equiv \boldsymbol{t} + \sum_{\boldsymbol{\alpha} > \boldsymbol{0}} \left((\boldsymbol{h}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \boldsymbol{g}' - (\boldsymbol{g}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \boldsymbol{h}'\right) \mod \mathfrak{m}^{\omega([\boldsymbol{g},\boldsymbol{h}]) + \min\{\omega(\boldsymbol{g}), \omega(\boldsymbol{h})\}+1}$$

that, since $\omega([\boldsymbol{g}, \boldsymbol{h}]) \geq \omega(\boldsymbol{g}) + \omega(\boldsymbol{h})$ and by Lemma 1.23, we can further approximate to

$$\begin{aligned} [\boldsymbol{g}, \boldsymbol{h}] &\equiv \boldsymbol{t} + \sum_{l=1}^n \left(h_l \partial_{\boldsymbol{\epsilon}_l} \boldsymbol{g}' - g_l \partial_{\boldsymbol{\epsilon}_l} \boldsymbol{h}'\right) \qquad \mod \mathfrak{m}^{\omega(\boldsymbol{h}) + \omega(\boldsymbol{g}) + \min\{\omega(\boldsymbol{f}), \omega(\boldsymbol{g})\}+1} \\ &\equiv \boldsymbol{t} + \sum_{l=1}^n \left(h_l \partial_{\boldsymbol{\epsilon}_l} \boldsymbol{g}' - g_l \partial_{\boldsymbol{\epsilon}_l} \boldsymbol{h}'\right) \qquad \mod \mathcal{G}\ell_n^{\omega(\boldsymbol{g}) + \omega(\boldsymbol{h})+1}(R). \end{aligned} \tag{2.2}$$

For every $j \in \mathbb{N}$, let μ_j denote the function from $\mathcal{G}\ell_n^j(R) / \mathcal{G}\ell_n^{j+1}(R)$ to $\hom_j$ that maps each $\boldsymbol{g} = (t_i + g_i)_{i=1}^n \mathcal{G}\ell_n^{j+1}(R)$ in $\mathcal{G}\ell_n^j(R) / \mathcal{G}\ell_n^{j+1}(R)$ to the homogeneous derivation $\sum_{i=1}^n \lfloor g_i \rfloor_{j+1} \partial_i$, where — for every $k \in \mathbb{N}$ and every $f = \sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}} \in R[\![\boldsymbol{t}]\!]$ — we use $\lfloor f \rfloor_k$ to denote the truncated polynomial $\sum_{|\boldsymbol{\alpha}| \leq k} f_\alpha \boldsymbol{t}^{\boldsymbol{\alpha}}$. Then μ_j can be seen to be a (topological) isomorphism of (topological) abelian groups (see formula (1.8)) and therefore the map $\mu : L(\mathcal{G}\ell_n^1(R)) \to \mathrm{Der}_R^1(R[\![\boldsymbol{t}]\!])$ defined by

$$\mu(\sum_{j>0} \boldsymbol{g} \mathcal{G}\ell_n^{j+1}(R)) := \sum_{j>0} \mu_j(\boldsymbol{g} \mathcal{N}_{j+1})$$

is in turn a (topological) group isomorphism. Moreover, by equation (2.2), the function μ turns out to be a continuous *anti*-isomorphism of Lie rings.

Notation 15. From now on, we identify $L(\mathcal{G}\ell_n^1(R))$ with $\mathrm{Der}_R^1(R[\![\boldsymbol{t}]\!])$, where the latter is seen as a Lie ring. So in particular, the map $\iota_{\mathcal{G}\ell_n^1(R)}$ defined in the previous section will be implicitly meant to be defined from $\mathcal{G}\ell_n^1(R)$ to $\mathrm{Der}_R^1(R[\![\boldsymbol{t}]\!])$. Agreeing to this convention, the image of $\boldsymbol{g} = (t_i + g_i)_{i=1}^n$ through $\iota_{\mathcal{G}\ell_n^1(R)}$ is $\sum_{i=1}^n \lfloor g_i \rfloor_{\omega(\boldsymbol{g})+1} \partial_i$. It is clear that $L_{\mathcal{G}\ell_n^1(R)}(\mathcal{G}\ell_n^i(R)) = \mathrm{Der}_R^i(R[\![\boldsymbol{t}]\!])$ for every $i \in \mathbb{N}$.

Remark 2.11. We stress the fact that the natural structure of $L(\mathcal{G}\ell_n^1(R))$ is the one of Lie-ring — i. e. of $\mathbb{Z}$-module with a Lie brackets operation —, whereas the structure of R-module — and thus of Lie R-algebra — is imposed *a fortiori*, in that there is no operation in $\mathcal{G}\ell_n^1(R)$ that corresponds to the multiplication by an element of R. However, in forgetting the R-module structure, we certainly do not lose the R-linearity of Lie brackets, and such a fact will turn out to be quite useful, later on.

Proposition 2.12. *Assume R is either a $\mathbb{Q}$-algebra, an $\mathbb{F}_p$-algebra or a $\mathbb{Z}_p$-algebra for some odd prime p and suppose $n > 1$. Then, for every $m, r \in \mathbb{N}$, the closure of the subgroup $[\mathcal{G}\ell_n^m(R), \mathcal{G}\ell_n^r(R)]$ equals $\mathcal{G}\ell_n^{m+r}(R)$.*

Proof. We prove this proposition only for $\mathbb{F}_p$-algebras, as it is the case of most interest for this thesis. However the other cases are completely analogous.

One inclusion has been already discussed. We prove the converse by making use of the associated algebra, namely proving that $\mathrm{Der}_R^{m+r}(R[\![\boldsymbol{t}]\!]) \subseteq [\mathrm{Der}_R^m(R[\![\boldsymbol{t}]\!]), \mathrm{Der}_R^r(R[\![\boldsymbol{t}]\!])]$. Indeed, by Proposition 2.10, it suffices to show that for every $\boldsymbol{\gamma} \in {\mathbb{N}_0}^n$ of weight $m + r + 1$ and every $i \in \{1, \ldots, n\}$, the derivation $\boldsymbol{t}^{\boldsymbol{\gamma}} \partial_i$ belongs to the $\mathbb{F}_p$-vector subspace spanned by

$$\left\{ \left[\boldsymbol{t}^{\boldsymbol{\alpha}} \partial_j, \boldsymbol{t}^{\boldsymbol{\beta}} \partial_k \right] \mid \boldsymbol{\alpha}, \boldsymbol{\beta} \in {\mathbb{N}_0}^n,\ |\boldsymbol{\alpha}| = m + 1,\ |\boldsymbol{\beta}| = r + 1,\ j, k \in \{1, \ldots, n\} \right\}.$$

The claim then follows from the R-linearity of the Lie brackets.

Suppose that $\boldsymbol{\gamma} \geq \boldsymbol{\epsilon}_j$ for some $j \neq i$, that is to say there exists $\boldsymbol{\gamma}'$ in ${\mathbb{N}_0}^n$ such that $\boldsymbol{\gamma} = \boldsymbol{\gamma}' + \boldsymbol{\epsilon}_j$. Let $\boldsymbol{\alpha}' = (\alpha'_l)_{l=1}^n$ and $\boldsymbol{\beta}' = (\beta'_l)_{l=1}^n$ be n-tuples in ${\mathbb{N}_0}^n$ of weights m and r respectively, whose sum $\boldsymbol{\alpha}' + \boldsymbol{\beta}'$ equals $\boldsymbol{\gamma}'$. Then, taking $\boldsymbol{\alpha} = \boldsymbol{\alpha}' + \boldsymbol{\epsilon}_i$ and $\boldsymbol{\beta} = \boldsymbol{\beta}' + \boldsymbol{\epsilon}_j$ if $\beta'_i - \alpha'_i \not\equiv_p 1$, or $\boldsymbol{\alpha} = \boldsymbol{\alpha}' + \boldsymbol{\epsilon}_j$ and $\boldsymbol{\beta} = \boldsymbol{\beta}' + \boldsymbol{\epsilon}_i$ otherwise, we have $\left[\boldsymbol{t}^{\boldsymbol{\alpha}} \partial_i, \boldsymbol{t}^{\boldsymbol{\beta}} \partial_i \right] = (\beta_i - \alpha_i) \boldsymbol{t}^{\boldsymbol{\gamma}} \partial_i \neq 0$.

So it only remains to prove the case $\boldsymbol{\gamma} = (m + r + 1)\boldsymbol{\epsilon}_i$. Fix $j \in \{1, \ldots, n\} \setminus \{i\}$. Then

$$\left[t_i^{m+1} \partial_j, t_i^r t_j \partial_i \right] = t_i^{m+r+1} \partial_i - (m+1) t_i^{m+r} t_j \partial_j$$

where $(m+1) t_i^{m+r} t_j \partial_j$ belongs to the subspace because of the first part of this proof. □

Remark 2.13. The hypothesis $n > 1$ is essential. Indeed it is known that when n is 1 and R is a finite field, this result does not hold; see [11, Theorem 2].

Corollary 2.14. *Let R be either a $\mathbb{Q}$-algebra, a $\mathbb{Z}_p$-algebra or an $\mathbb{F}_p$-algebra for some odd prime p and suppose $n > 1$. Then $\{\mathcal{G}\ell_n^i(R) \mid i \in \mathbb{N}\}$ is the lower central series of $\mathcal{G}\ell_n^1(R)$.*

Corollary 2.15. *Let n be at least 2. The generalized Nottingham group of rank n over a finite field $\mathbb{F}_q$ of odd characteristic p is a pro-p group finitely generated by $n|\mathbb{F}_q : \mathbb{F}_p|\binom{n+1}{n-1}$ elements.*

Proof. The generalized Nottingham group over $\mathbb{F}_q$ is a a pro-p group by Proposition 1.33. Proposition 2.12 and Corollary 1.22 imply that the Frattini subgroup of $\mathcal{G}\ell_n^1(\mathbb{F}_q)$ is $\mathcal{G}\ell_n^2(\mathbb{F}_q)$. By Corollary 1.20, the $\mathbb{F}_p$-dimension of $\mathcal{G}\ell_n^1(\mathbb{F}_q) / \mathcal{G}\ell_n^2(\mathbb{F}_q)$ is $n|\mathbb{F}_q : \mathbb{F}_p|\binom{n+1}{n-1}$. □

Remark 2.16. The latter corollary is indeed a particular case of a more general result. What we actually proved in Proposition 2.12, is that the additive subgroup generated by $[\mathrm{hom}_i, \mathrm{hom}_j]$

is $\hom_{i+j}$ for every positive integers i, j (where $\hom_i$ is the set of homogeneous derivations of degree $i+1$ defined in Remark 2.2). This implies that in the hypothesis of the proposition, the set $\hom_1$ topologically generate $\mathrm{Der}^1_R(R[\![\boldsymbol{t}]\!]) = L(\mathcal{G}\ell^1_n(R))$ as a Lie ring. Thus, using Proposition 2.10, we obtain that $\{\boldsymbol{t} + r\boldsymbol{t}^{\boldsymbol{\alpha}}\boldsymbol{E}_i \mid r \in R,\ |\boldsymbol{\alpha}| = 2,\ i \in \{1, \ldots, n\}\}$ is a set of (topological) generators for $\mathcal{G}\ell^1_n(R)$.

Part II

Cartan type and other subgroups

Chapter 3

Cartan type subgroups

As already said in the introduction to this thesis, A. Shalev introduced [34] the generalized Nottingham group with the main purpose of finding new just infinite pro-p groups. We will deal the just infiniteness of the generalized Nottingham group in more details in Chapter 6, however the feeling was that also some interesting subgroups of the Nottingham group may be just infinite, namely the Cartan type pro-p groups. The name of this family of subgroups is due to their construction, related to Cartan type subalgebras of the Witt algebra.

When dealing with dimensions higher than one, by Witt algebras authors might mean different — although strictly related — definitions. Usually — for instance in [6], our main reference for the subject —, for a positive integer m, the n-th Witt algebra $W(n:\mathbf{1})$ is the restricted simple Lie algebra of derivations of $\mathrm{Der}_{\mathbb{F}_p}\left((\mathbb{F}_p[\boldsymbol{t}]/(t_1^p,\dots,t_n^p))\right)$, but it can be seen as a particular subalgebra of the algebra $W(m)$ of special derivations of the completed algebra of divided powers; see [6, 38].

The other Cartan type algebras are subalgebras of the Witt algebra that annihilate some differential form; however, again, they can also be seen as particular subalgebras of a larger subalgebra of $W(m)$.

From the previous chapter, we know that the Lie algebra associated to $\mathcal{G}\ell_n^1(\mathbb{F}_p)$ is a subalgebra of $\mathrm{Der}_{\mathbb{F}_p}(\mathbb{F}_p[\![\boldsymbol{t}]\!])$ (reversing order). Indeed the n-th Witt algebra is a quotient of $\mathrm{Der}_{\mathbb{F}_p}(\mathbb{F}_p[\![\boldsymbol{t}]\!])$ (see also Example 5.3).

In what follows we explicit the — supposed — basic idea of Shalev constructing analogous of Cartan type subalgebras (or better: their extended version) where the starting point is the formal power series algebra, instead of the completed divided powers algebra. However our construction remains quite general, not depending on the ring R.

The construction of Cartan type algebras given by Block and Wilson [6] will be followed.

3.1 The exterior algebra of differential forms

The automorphism group of $R[\![\boldsymbol{t}]\!]$ acts on $\mathrm{Der}(R[\![\boldsymbol{t}]\!])$ by $\phi(D)(g)=\phi(D(\phi^{-1}(g)))$ for every $D\in\mathrm{Der}_R(R[\![\boldsymbol{t}]\!])$, $\phi\in\mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$ and $g\in R[\![\boldsymbol{t}]\!]$.

Consider the set of $R[\![\boldsymbol{t}]\!]$-module morphisms $\mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}_R(R[\![\boldsymbol{t}]\!]),R[\![\boldsymbol{t}]\!])$. It has a natural structure of $R[\![\boldsymbol{t}]\!]$-module and we make $\mathrm{Der}_R(R[\![\boldsymbol{t}]\!])$ act on it by

$$(D(\Phi))(E):=D(\Phi(E))-\Phi([D,E]) \tag{3.1}$$

for every $D, E \in \mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right)$ and $\Phi \in \mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$. Note also that

$$\begin{aligned} D(f\Phi)(E) = D(f\Phi(E)) - f\Phi([D,E]) = D(f)\Phi(E) + fD(\Phi(E)) - f\Phi([D,E]) = \\ = D(f)\Phi(E) + fD(\Phi)(E) \end{aligned}$$

for every $f \in R[\![\boldsymbol{t}]\!]$.

Let $\mathrm{d} : R[\![\boldsymbol{t}]\!] \to \mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$ be such that $\mathrm{d}f(D) = D(f)$ for every derivation D and every formal power series f. Then for every $\Phi \in \mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$ and every derivation $D = \sum_{i=1}^n D_i\partial_i \in \mathrm{Der}\left(R[\![\boldsymbol{t}]\!]\right)$ we have

$$\Phi(D) = \Phi(\sum_{i=1}^n D_i\partial_i) = \sum_{i=1}^n D_i\Phi(\partial_i) = \sum_{i=1}^n \Phi(\partial_i)\mathrm{d}t_i(D)$$

whence we deduce that $\mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$ is a free $R[\![\boldsymbol{t}]\!]$-module — a base for which is given by $\mathrm{d}t_1, \ldots, \mathrm{d}t_n$ — as for every $a_1, \ldots, a_n$ in $R[\![\boldsymbol{t}]\!]$, the homomorphism $\sum_{i=1}^n a_i\mathrm{d}t_i$ applied to ∂_j gives a_j and therefore it is the trivial homomorphism if and only if $a_j = 0$ for every $j \in \{1, \ldots, n\}$. Moreover, applying definition (3.1),

$$D(\mathrm{d}f)(E) = DE(f) - [D,E]\,(f) = ED(f) = \mathrm{d}(Df)(E)$$

that is $D(\mathrm{d}f) = \mathrm{d}(Df)$, for every $D, E \in \mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right)$ and every $f \in R[\![\boldsymbol{t}]\!]$.

Let Ω be the exterior algebra of $\mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$. Then Ω is a free $R[\![\boldsymbol{t}]\!]$-module, a base for which is given by $\{\mathrm{d}t_{j_1} \wedge \mathrm{d}t_{j_2} \cdots \wedge \mathrm{d}t_{j_s} \mid \{j_1 < j_2 < \ldots < j_s\} \subseteq \{1, \ldots, n\}\}$. We can extend any $D \in \mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right)$ to a derivation of Ω by imposing, for every $\omega, \lambda \in \Omega$,

$$D(\omega \wedge \lambda) = D(\omega) \wedge \lambda + \omega \wedge D(\lambda)$$

and $D(f\lambda) = D(f)\lambda + fD(\lambda)$ for every $f \in R[\![\boldsymbol{t}]\!]$.

Finally $\mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$ acts on $\mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$ by

$$\phi(\Phi)(D) = \phi^{-1}(\Phi(\phi(D)))$$

— for every $\phi \in \mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$, $\Phi \in \mathrm{Hom}_{R[\![\boldsymbol{t}]\!]}(\mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right), R[\![\boldsymbol{t}]\!])$ and $D \in \mathrm{Der}_R\left(R[\![\boldsymbol{t}]\!]\right)$ — and we can naturally extend the action to Ω. In particular the image of $\lambda \wedge \omega$ through an automorphism $\phi \in \mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$ equals $\phi(\lambda) \wedge \phi(\omega)$ for all λ, ω in Ω and — for every formal power series f and every derivation D —

$$\phi(\mathrm{d}f)(D) = \phi^{-1}(\mathrm{d}f(\phi(D))) = \phi^{-1}(\phi(D)(f)) = \phi^{-1}(\phi(D(\phi^{-1}(f)))) = D\phi(f) = \mathrm{d}\phi(f)(D),$$

that is

$$\phi(\mathrm{d}f) = \mathrm{d}(\phi(f)). \tag{3.2}$$

Consider the following differential forms:

- $\omega_S := \mathrm{d}t_1 \wedge \ldots \wedge \mathrm{d}t_n$;
- $\omega_H := \sum_{i=1}^r \mathrm{d}t_i \wedge \mathrm{d}t_{i+r}$ for $n = 2r$;
- $\omega_K := \mathrm{d}t_{2r+1} + \sum_{i=1}^r (t_{i+r}\mathrm{d}t_i - t_i\mathrm{d}t_{i+r})$ for $n = 2r + 1$.

We define the special algebra $S_n(R)$ and the hamiltonian algebra $H_n(R)$ to be the annihilator algebras of ω_S and ω_H respectively; the contact algebra $K_n(R)$ is the algebra of derivations D such that $D(\omega_K) \in R[\![\boldsymbol{t}]\!]\omega_K$. These are the Cartan type subalgebras of $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$.

On the other side, the special group and the hamiltonian group are defined to be stabilizer subgroups in $\operatorname{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ of ω_S, and ω_H respectively; the contact group instead is the group of automorphisms $\phi \in \operatorname{Aut}^1_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ such that $\phi(\omega_K)$ is in the submodule $R[\![\boldsymbol{t}]\!]\omega_K$. We call these groups Cartan type subgroups of the generalized Nottingham group.

We will mostly work with the corresponding subgroups of $\mathcal{Gl}^1_n(R)$, denoted by $\mathcal{Sl}^1{}_n(R)$, $\mathcal{H}^1{}_n(R)$ and $\mathcal{K}^1{}_n(R)$ respectively.

The main question about these groups is whether — over a finite field — they are just infinite or not. We do not have an answer, however in the next section we start the study of the simplest among these, the Special subgroup, and in Chapter 8 we show a concrete possible way for a proof.

3.2 The Special subgroup over a finite field

Proposition 3.1. *The elements of the special algebra $S_n(R)$ are those derivations in $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ whose divergence is null.*

Definition. We define the divergence to be the function

$$\operatorname{div} : \operatorname{Der}_R(R[\![\boldsymbol{t}]\!]) \to R[\![\boldsymbol{t}]\!]$$

such that $\operatorname{div}(\sum_{i=1}^n f_i \partial_i) = \sum_{i=1}^n \partial_i f_i$.

Remark 3.2. Divergence is in fact an homomorphism of R-modules.

Remark 3.3. A base for the free R-module underlying $\operatorname{Der}_R(R[\![\boldsymbol{t}]\!])$ is given by $\{\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i \mid i \in \{1,\dots,n\},\ \boldsymbol{\alpha} \in {\mathbb{N}_0}^n\}$ and the image through divergence function of $\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i$ is $\alpha_i \boldsymbol{t}^{\boldsymbol{\alpha}-\boldsymbol{\epsilon}_i}$, therefore there exists an R-base of Im(div) that is a subbase of $\{\boldsymbol{t}^{\boldsymbol{\alpha}}\}$. In particular, to compute the rank of Im(div) it will suffices to count n-tuples $\boldsymbol{\alpha}$ such that $\boldsymbol{t}^{\boldsymbol{\alpha}} \in \operatorname{Im}(\operatorname{div})$.

Proof of Proposition 3.1. Let $D = \sum_{i=1}^n f_i \partial_i$ be a derivation. Then

$$\begin{aligned} D(\omega_S) =& D(\mathrm{d}t_1) \wedge \mathrm{d}t_2 \wedge \cdots \wedge \mathrm{d}t_n + \mathrm{d}t_1 \wedge D(\mathrm{d}t_2) \wedge \cdots \wedge \mathrm{d}t_n + \cdots + \mathrm{d}t_1 \wedge \mathrm{d}t_2 \wedge \cdots \wedge D(\mathrm{d}t_n) \\ =& \mathrm{d}(f_1) \wedge \mathrm{d}t_2 \wedge \cdots \wedge \mathrm{d}t_n + \mathrm{d}t_1 \wedge \mathrm{d}(f_2) \wedge \cdots \wedge \mathrm{d}t_n + \cdots + \mathrm{d}t_1 \wedge \mathrm{d}t_2 \wedge \cdots \wedge \mathrm{d}(f_n) \\ =& (\partial_1 f_1)\omega_S + (\partial_2 f_2)\omega_S + \cdots + (\partial_n f_n)\omega_S \\ =& \operatorname{div}(D)\omega_S \end{aligned}$$

yielding the claim. □

For every integer $x \geq -1$ let $h_x(S_n(R))$ denote $S_n(R) \cap \hom_x$ (where $\hom_x$ is the set of homogeneous derivations, see Remark 2.2). Then $S_n(R) = \bigoplus_{x \geq -1} h_x(S_n(R))$ is a graded algebra.

Corollary 3.4. *Assume R is a field of characteristic p. For every $x \geq -1$,*

$$\dim_R h_x(S_n(R)) = \binom{n+x}{n-1} \times n - \binom{n+x-1}{n-1} + \varepsilon(x)$$

where $\varepsilon(x) = \binom{x'+n-1}{n-1}$ if $x = x'p + n(p-1)$ for some $x' \in \mathbb{N}_0$, otherwise $\varepsilon(x) = 0$.

Proof. Consider the R-linear application

$$\operatorname{div}_x = \operatorname{div}|_{\operatorname{hom}_x} : \operatorname{hom}_x \to \bigoplus_{|\boldsymbol{\alpha}|=x} R\boldsymbol{t}^{\boldsymbol{\alpha}}$$

that is just the restriction of div to hom_x. Let $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$ be an n-tuple of weight $|\boldsymbol{\alpha}| = x$. If there exists $j \in \{1, \dots, n\}$ such that $\alpha_j \not\equiv_p -1$, then $\operatorname{div}_x(R\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_j}\partial_j) = R\boldsymbol{t}^{\boldsymbol{\alpha}}$. Actually an R-base of $\operatorname{Im}(\operatorname{div}_x)$ is given by $\{\boldsymbol{t}^{\boldsymbol{\alpha}} \mid |\boldsymbol{\alpha}| = x$ and there exists $j \in \{1, \dots, n\}$ such that $\alpha_j \not\equiv_p -1\}$.

If there exists no x' such that $x = x'p+n(p-1)$, then there exists no $\boldsymbol{\alpha}$ of weight x such that $\boldsymbol{t}^{\boldsymbol{\alpha}}$ is not in the just mentioned set and therefore div_x is surjective, otherwise there are $\binom{x'+n-1}{n-1}$ such $\boldsymbol{\alpha}$. Hence the claim, as $\dim_R(h_x(S_n(R))) = \dim_R \ker(\operatorname{div}_x) = \dim_R(\operatorname{hom}_x) - \dim_R \operatorname{Im}(\operatorname{div}_x)$. □

Proposition 3.5. *The special group is formed by elements $\boldsymbol{f}$ in $\mathcal{G}\ell^1_n(R)$ whose Jacobian has determinant equal to* 1.

Proof. It is just a matter of direct computations. Let $\boldsymbol{f}$ be in $\mathcal{G}\ell^1_n(R)$ and let ϕ be the corresponding automorphism in $\operatorname{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$. Then, by equation (3.2),

$$\begin{aligned}\phi(\omega_S) &= \mathrm{d}\phi(t_1) \wedge \cdots \wedge \mathrm{d}\phi(t_2) = (\sum_{i=1}^n \partial_i\phi(t_1)\mathrm{d}t_i) \wedge \cdots \wedge (\sum_{i=1}^n \partial_i\phi(t_n)\mathrm{d}t_i)\\ &= \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n \partial_{i_1}\phi(t_1)\cdots\partial_{i_n}\phi(t_n)\mathrm{d}t_{i_1} \wedge \cdots \wedge \mathrm{d}t_{i_n}\\ &= \det(\partial_i\phi(t_j))_{i,j=1}^n\omega_S = \det(\operatorname{Jac}\boldsymbol{f})\omega_S\end{aligned}$$

Hence the claim follows. □

Corollary 3.6. *The special group $\mathcal{S}\ell^1{}_n(R)$ is closed in $\mathcal{G}\ell^1_n(R)$.*

Corollary 3.7. *The intersection of the special algebra $S_n(R)$ with $\operatorname{Der}^1_R(R[\![\boldsymbol{t}]\!])$ is isomorphic to $L(\mathcal{S}\ell^1{}_n(R))$.*

Proof. Recall that for every $f \in R[\![\boldsymbol{t}]\!]$, we denote by $\lfloor f \rfloor_r$ the lowest degree representative of $f + \mathfrak{m}^{r+1}$.

Let $\boldsymbol{f} = (t_i + f_i)_{i=1}^n$ be in $\mathcal{G}\ell^1_n(R)$. Then

$$\det\operatorname{Jac}(\boldsymbol{f}) = 1 + \sum_{i=1}^n \partial_i f_i + F((\partial_i f_j)_{i,j=1}^n)$$

where $F \in R[X_{1,1}, \dots, X_{n,n}]$ is a polynomial of order at least 2. In particular, for every $r \in \mathbb{N}$

$$\det\operatorname{Jac}(\boldsymbol{f}) \equiv 1 + \sum_{i=1}^n \partial_i\lfloor f_i\rfloor_{\omega(\boldsymbol{f})+r} + F((\partial_i\lfloor f_j\rfloor_{\omega(\boldsymbol{f})+r-1})_{i,j=1}^n) \mod \mathfrak{m}^{\omega(\boldsymbol{f})+r+1}$$

whence $\boldsymbol{f}$ is in $\mathcal{S}\ell^1{}_n(R)$ if and only if $\sum_{i=1}^n \partial_i\lfloor f_i\rfloor_{\omega(\boldsymbol{f})+r} = -\lfloor F((\partial_i\lfloor f_j\rfloor_{\omega(\boldsymbol{f})+r-1})_{i,j=1}^n)\rfloor_{\omega(\boldsymbol{f})+r-1}$ for every $r \in \mathbb{N}$. It follows that if $\boldsymbol{f}$ is in $\mathcal{S}\ell^1{}_n(R)$, then $\sum_{i=1}^n \partial_i\lfloor f_i\rfloor_{\omega(\boldsymbol{f})+1} = 0$ and, conversely, for any n-tuple $(g_i)_{i=1}^n$ of homogeneous polynomials of degree x there exists an n-tuple $\boldsymbol{f}' = (f'_i)_{i=1}^n$ such that $\lfloor f'_i\rfloor_x = g'_i$ for every $i \in \{1, \dots, n\}$ and $\det\operatorname{Jac}(\boldsymbol{t} + \boldsymbol{f}) = 1$. Now the claim follows since the divergence of a formal power series is 0 if and only if it is 0 on each homogeneous component. □

Now, let R be a finite field of characteristic p. We are going to exhibit a (infinite) set of R-generators for $S_n(R)$. We start defining the following subsets:

$$\begin{aligned} A \quad &:= \{\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i \in S \mid \boldsymbol{\alpha} \in {\mathbb{N}_0}^n, i \in \{1, \dots, n\} \text{ s. t. } \alpha_i \equiv_p 0\} \\ B \quad &:= \big\{(\alpha_j + 1)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_i}\partial_i - (\alpha_i + 1)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_j}\partial_j \in S \mid \boldsymbol{\alpha} \in {\mathbb{N}_0}^n, i, j \in \{1, \dots, n-1\} \text{ s. t.} \\ &\qquad\qquad \alpha_i \not\equiv_p -1 \text{ and } \exists j = \min_{\{1,\dots,n\}} \{k > i \mid \alpha_k \not\equiv_p -1\}\big\} \\ C \quad &:= A \cup B \end{aligned}$$

Proposition 3.8. *Let R be a field of characteristic p. For every $x \geq -1$, the set $C_x = C \cap h_x(S_n(R))$ is an R-base of $h_x(S_n(R))$.*

Proof. Consider the function ξ from C_x to the set P_x of pairs $(\boldsymbol{\alpha}, i) \in {\mathbb{N}_0}^n \times \{1, \dots, n\}$ such that $\boldsymbol{\alpha}$ has weight $x+1$ defined by $\xi(\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i) = (\boldsymbol{\alpha}, i)$ on $A \cap C_x$ and by $\xi((a_j+1)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_i}\partial_i - (a_i+1)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_j}\partial_j) = (\boldsymbol{\alpha} + \boldsymbol{\epsilon}_i, i)$ on $B \cap C_x$: it is well defined since A and B have empty intersection. The pair $(\boldsymbol{\alpha}, i)$, where $\boldsymbol{\alpha} = (\alpha_j)_{j=1}^n$, is not in the image of ξ if and only if $\alpha_i \not\equiv_p 0$ and there exists no $j \in \{i+1, \dots, n\}$ such that $\alpha_j \not\equiv -1$. So we can define a function Ξ from $P_x \setminus \mathrm{Im}(\xi)$ to $R[\![\boldsymbol{t}]\!]$ sending $(\boldsymbol{\alpha}, i)$ to $\boldsymbol{t}^{\boldsymbol{\alpha}-\boldsymbol{\epsilon}_i}$. Let $(\boldsymbol{\alpha}, i)$ and $(\boldsymbol{\beta}, j)$ be in $P_x \setminus \mathrm{Im}(\xi)$ having the same image through Ξ. Then if j was greater than i — or vice versa —, we would have that $\beta_j - 1$ should be equivalent modulo p to -1, whereas we know that β_j is not equivalent to 0. So $i = j$ and therefore $\boldsymbol{\alpha} = \boldsymbol{\beta}$ since $\boldsymbol{\alpha} - \boldsymbol{\epsilon}_i = \boldsymbol{\beta} - \boldsymbol{\epsilon}_j$. In other words, the function Ξ is injective. Moreover an element $\boldsymbol{t}^{\boldsymbol{\alpha}}$ is in the image of Ξ for an n-tuple $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^n$ only if α_i is not equivalent to -1 modulo p for some $i \in \{1, \dots, n\}$ and therefore only if $\boldsymbol{t}^{\boldsymbol{\alpha}}$ is an element of the base of the image of div_x (see the proof of Corollary 3.4). Thus

$$|C_x| + \dim_R \mathrm{Im}(\mathrm{div}_x) \geq |C_x| + \mathrm{Im}(\Xi) \geq |P_x| = \dim_R \hom_x$$

whence $|C_x| \geq \dim_R h_x(S_n(R))$. It remains to prove that elements of C_x are linearly independent. It is clear that so they are elements of A_x and that the intersection of the subspace generated by A_x trivially intersect the subspace generated by B_x, so it suffices to prove that elements of B_x are linearly independent. We may endow B_x of a partial order as follows. Let b_1 and b_2 be elements of B_x and let $(\boldsymbol{\alpha}_1, i_1)$ and $(\boldsymbol{\alpha}_2, i_2)$ their image through ξ, then $b_1 \preceq b_2$ if and only if $i_1 \leq i_2$. Note that if $b_1 \leq b_2$ and $b_2 \leq b_1$, then either $b_1 = b_2$ or $\xi(b_1)$ and $\xi(b_2)$ are different. So assume $\sum_{b \in B_x} r_b b = 0$ for some $(r_b)_{b \in B_x} \in R^{B_x}$ and suppose there exists $b \in B_x$ such that r_b is not zero. Assume furthermore that $b = (\alpha_j + 1)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_i}\partial_i - (\alpha_i + 1)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_j}\partial_j$ is minimal with this property with respect to the just defined order. Then $\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\epsilon}_i}\partial_i$ does not appear as component of any other $b \in B_x$ such that $r_b \neq 0$ and therefore does not cancel out in the summation, contradicting the assumption $\sum_{b \in B_x} r_b b = 0$. □

Let Γ be an $\mathbb{F}_p$-base of R. Then from Proposition 2.10 we obtain

Corollary 3.9. *Let R be as before. Let $U \subseteq {\mathcal{S}\ell^1}_n(R)$ be such that for every $D \in C \cap \mathrm{Der}_R^1(R[\![\boldsymbol{t}]\!])$ and every $a \in \Gamma$ there exists $\boldsymbol{f} \in U$ whose image through $\iota_{\mathcal{G}\ell_n^1(R)}$ is aD. Then U generate ${\mathcal{S}\ell^1}_n(R)$*

Such a set exists, as shown in the proof of Corollary 3.7.

Chapter 4

Pseudo-algebraic subgroups

This chapter is an exploratory introduction to a family of subgroups of $\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$ that seem to have very nice properties and might be a very good tool to study Cartan type subgroups. Still, everything is at a very low stage and the interest for this subject is, so far, mostly based on speculations, some of which are discussed in the conclusive chapter. The reader, willing to have more information about this regard or unsatisfied by the sudden end of this chapter, is invited to look at the last section of Chapter 8.

The reading of this chapter should also clarify the reasons for our notation for groups of n-tuples in the ring of formal power series under substitution.

In what follows K is a fixed ring (possibly, but not necessarily, a field).

4.1 Basic introduction to linear algebraic groups

A very basic background on linear algebraic groups is needed. Our main reference for the subject is Waterhouse's book [41], however here we recall main definitions and results that are necessary for the chapter.

An affine algebraic group over K is — by definition — a representable functor $\mathbb{G}$ from the category of K-algebras to the category of groups. Representable functor means that there exists a K-algebra A such that $\mathbb{G}(V) = \mathrm{Hom}_K(A, V)$ for every K-algebra V. It turns out that the representing K-algebras has some additional structure, namely it is an Hopf algebra.

Definition. An Hopf K-algebra A is a commutative K-algebra endowed with the K-algebra maps

$$\begin{aligned} \text{comultiplication} \qquad \Delta :& A \to A \otimes A \\ \text{counit} \qquad \varepsilon :& A \to K \\ \text{coinverse} \qquad S :& A \to A \end{aligned}$$

such that the diagrams

$$\begin{tikzcd} A \otimes A \otimes A & A \otimes A \arrow[l, "\mathrm{id} \otimes \Delta"'] \\ A \otimes A \arrow[u, "\Delta \otimes \mathrm{id}"] & A \arrow[l, "\Delta"] \arrow[u, "\Delta"'] \end{tikzcd} \qquad \begin{tikzcd} K \otimes A & A \otimes A \arrow[l, "\mathrm{id} \otimes \Delta"'] \\ A \arrow[u, phantom, "\wr\Vert"] \arrow[r, phantom, "="] & A \arrow[u, "\Delta"'] \end{tikzcd} \qquad \begin{tikzcd} A & A \otimes A \arrow[l, "(S, id)"'] \\ K \arrow[u] & A \arrow[l, "\varepsilon"'] \arrow[u, "\Delta"'] \end{tikzcd}$$

commute.

Remark 4.1. Some authors use different definition of Hopf algebra, for example they might be non-commutative.

Indeed the relation that associates an algebraic group to its Hopf algebra is a contravariant functor.

Example 4.1. The general linear group over K is the functor GL_n represented by the algebra $A_{\mathrm{GL}_n} := K[X_{1,1}, \dots, X_{n,n}, Y]/I_{\mathrm{GL}_n}$ where I_{GL_n} is the ideal generated by $Y \det(X_{i,j})_{j,i=1}^n - 1$ where $\det(X_{i,j})_{j,i=1}^n$ is the polynomial formula to compute the determinant of an $n \times n$ matrix. In this case comultiplication is given by $\Delta(X_{i,j}) = \sum_{l=1}^n X_{i,l} \otimes X_{l,j}$.

An homomorphism of affine group schemes over K corresponds to Hopf algebras homomorphisms, that is K-algebras homorphisms that preserve Δ. In particular a surjective homomorphism of Hopf algebras corresponds to an embedding (called closed embedding) of algebraic groups over K. Hence a closed subgroup $\mathbb{H}$ of $\mathbb{G}$ is the functor represented by a quotient algebra A/I of the Hopf algebra A associated to $\mathbb{G}$. As A/I must be in turn an Hopf algebra, the ideal I has to satisfy some conditions:

$$\Delta(I) \subseteq I \otimes A + A \otimes I, \quad S(I) \subseteq I, \quad \varepsilon(I) = 0 \tag{4.1}$$

If this is the case we say that I is an Hopf ideal.

Definition. A linear algebraic group is defined to be a closed subgroup of GL_n.

From what we said we deduce that a linear algebraic group is represented by an Hopf algebra of the kind $K[X_{1,1}, \dots, X_{n,n}, Y]/I$ where I is an Hopf ideal containing the one generated by $Y \det(Xi,j)_{j,i=1}^n - 1$.

When we evaluate a linear algebraic group $\mathbb{G}$ on some K-algebra V we are taking the set $\mathrm{Hom}_K(A, V)$ and every homomorphism ϕ in it is essentially determined by the images $\phi(X_{i,j}) \in V$ for every $X_{i,j}$ that need to satisfy the polynomials in I ($\phi(Y)$ is uniquely determined by images of other indeterminates). Thus we may represent every $\phi \in \mathrm{Hom}_K(A, V)$ by an $n \times n$ matrix $(\phi(X_{i,j}))_{i,j=1}^n$. Indeed $\mathrm{Hom}_K(A, V)$ is a group under the product defined by

$$\phi \cdot \psi(X_{i,j}) = (\phi, \psi)(\Delta(X_{i,j})) \quad \text{for all } \phi, \psi \in \mathrm{Hom}_K(A, V)$$

— where (ϕ, ψ) is the unique map $A \otimes A \to V$ that factorizes $a \times b \mapsto \phi(a)\phi(b)$ (it exists because of the universal property of $A \otimes A$) — and in the linear case the comultiplication Δ is induced by the comultiplication of GL_n and in particular the identification of $\mathbb{G}(V)$ with the matrices $n \times n$ is indeed a group isomorphism where we put the product of two matrices to be precisely the matrix multiplication.

Example 4.2. The special linear group SL_n over K is the functor represented by the quotient of the Hopf K-algebra A_{GL_n} over the ideal generated by $\det(X_{i,j})_{j,i=1}^n - 1$. Note that its Hopf algebra can also be seen as the quotient algebra of $K[X_{1,1}, \dots, X_{n,n}]$ over the ideal generated by the same polynomial $\det(X_{i,j})_{j,i=1}^n - 1$. It is a subgroup of GL_n and its evaluation on a K-algebra V corresponds to the subgroup of $\mathrm{GL}_n(V)$ of matrices whose determinant is 1.

Remark 4.2. Let $\mathbb{G}$ be a linear algebraic group embedded into GL_n and let V be a K-algebra. Since the matrices of $\mathbb{G}(V)$ are those satisfying a certain collection of polynomials, the group is closed under the product topology of V with itself $n \times n$ times.

4.2 Definition

Notation 16. Throughout the remaining of this chapter, the capital letter R denotes a K-algebra.

Definition. Let $\mathbb{G}$ be a linear algebraic group over K endowed with a fixed embedding into GL_n. A closed subgroup G of $\mathcal{G}\ell_n(R)$ is called pseudo-algebraic group over K evaluated on R associated to $\mathbb{G}$ if any $\boldsymbol{f} \in \mathcal{G}\ell_n(R)$ is in G if and only if $\mathrm{Jac}(\boldsymbol{f})$ is in $\mathbb{G}(R[\![\boldsymbol{t}]\!])$.

Example 4.3. The group $\mathcal{G}\ell_n(R)$ itself is a pseudo-algebraic subgroup over K evaluated on K associated to $\mathrm{GL}_n(R)$. In fact we proved (Corollary 1.16) that an n-tuple $\boldsymbol{f} \in \mathcal{M}_n(R)$ is in $\mathcal{G}\ell_n(R)$ if and only if its Jacobian is invertible.

Proposition 4.3. *For every closed embedding of a linear algebraic group $\mathbb{G}$ over K into GL_n, there exists a pseudo-algebraic subgroup associated to $\mathbb{G}$.*

Proof. Define

$$\mathcal{G}(R) := \{\boldsymbol{f} \in \mathcal{G}\ell_n(R)[\![\boldsymbol{t}]\!] \mid \mathrm{Jac}(\boldsymbol{f}) \in \mathbb{G}(R[\![\boldsymbol{t}]\!])\} \subseteq \mathcal{G}\ell_n(R) \tag{4.2}$$

We prove that it is a closed subgroup.

Let $\boldsymbol{f}, \boldsymbol{g} \in \mathcal{M}_n(R)$ be in $\mathcal{G}(R)$. Then, by the chain rule,

$$\mathrm{Jac}(\boldsymbol{f} \circ \boldsymbol{g}) = (\mathrm{Jac}(\boldsymbol{f}) \circ \boldsymbol{g}) \cdot \mathrm{Jac}(\boldsymbol{g}) \tag{4.3}$$

where $\mathrm{Jac}(\boldsymbol{g})$ is in $\mathbb{G}(R)$ by definition and the substitution $\mathrm{Jac}(\boldsymbol{f}) \circ \boldsymbol{g}$ is meant to be component-wise. Indeed, such a substitution coincides with a component-wise application of an automorphism $\Phi_{\boldsymbol{g}} \in \mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$. The resulting matrix corresponds to the morphism $A_{\mathbb{G}} \to R[\![\boldsymbol{t}]\!]$ given by the composition of the homomorphism $A_{\mathbb{G}} \to R[\![\boldsymbol{t}]\!]$ associated to $\mathrm{Jac}(\boldsymbol{f})$ with the automorphism $\Phi_{\boldsymbol{g}}$, in particular it lies in $\mathbb{G}(R[\![\boldsymbol{t}]\!])$. So, $\mathrm{Jac}(\boldsymbol{f}) \circ \boldsymbol{g}$ and $\mathrm{Jac}(\boldsymbol{g})$ are elements of the $n \times n$ matrix representation of $\mathbb{G}(R)$, but then their product is also in $\mathbb{G}(R)$ and therefore — by definition — $\boldsymbol{f} \circ \boldsymbol{g}$ lies in $\mathcal{G}_n(R)$. Similarly, solving equation (4.3) where we substitute $\boldsymbol{f}^{-1}$ to $\boldsymbol{g}$, we obtain

$$\mathrm{Jac}(\boldsymbol{f}^{-1}) = \left(\mathrm{Jac}(\boldsymbol{f}) \circ \boldsymbol{f}^{-1}\right)^{-1}$$

that — for analogous reasons to the previous ones — is in $\mathbb{G}(R)$.

Moreover, since Zariskii closed subsets of $(R[\![\boldsymbol{t}]\!])^{n\times n}$ are closed under the topology inherited from the topology of R, the set underlying the abstract group $\mathbb{G}(R[\![\boldsymbol{t}]\!])$ is closed in $\mathrm{GL}_n(R) \subseteq (R[\![\boldsymbol{t}]\!])^n$. Therefore $\mathcal{G}(R)$ is closed, being the pre-image of $\mathbb{G}(R)$ through the continuous function $\mathrm{Jac} : \mathcal{G}(R) \to \mathrm{GL}_n(R[\![\boldsymbol{t}]\!])$. □

Remark 4.4. A more direct approach to the proof that $\mathrm{Jac}(\boldsymbol{f}) \circ \boldsymbol{g}$ is in $\mathbb{G}(R[\![\boldsymbol{t}]\!])$ is the following. An $n \times n$ matrix with coefficients in $R[\![\boldsymbol{t}]\!]$ is in $\mathbb{G}(R[\![\boldsymbol{t}]\!])$ if and only if satisfies a set of polynomials $P \subseteq K[X_{11}, \ldots, X_{nn}]$. Let $p \in P$ be such a polynomial. Then $p \circ (\mathrm{Jac}(\boldsymbol{f}) \circ \boldsymbol{g}) = (p \circ \mathrm{Jac}\boldsymbol{f}) \circ \boldsymbol{g} = 0 \circ \boldsymbol{g} = 0$.

Example 4.4. The pseudo-algebraic subgroup $\mathcal{S}\ell_n(R)$ associated to SL_n is the group of n-tuples in $\mathcal{M}_n(R)$ whose Jacobian has determinant equal to 1. By Proposition 3.5, when we intersect it with $\mathcal{G}\ell_n^1(R)$ we find exactly the special subgroup of Cartan type.

Example 4.5. Let n equal 3 and let $\mathbb{U}_3$ be the Heisenberg group, i. e. the group of unipotent 3×3 matrices. Consider the associated pseudo-algebraic subgroup $\mathcal{U}_3(R)$. Then $\boldsymbol{f} = (t_i + f_i)_{i=1}^n \in \mathcal{G}\ell_n(R)$ is in $\mathcal{U}_3(R)$ if and only if there exist $a, b, c \in R[\![\boldsymbol{t}]\!]$ such that

$$\begin{pmatrix} 1 + \partial_1 f_1 & \partial_2 f_1 & \partial_3 f_1 & \\ \partial_1 f_2 & 1 + \partial_2 f_2 & \partial_3 f_2 & \\ \partial_1 f_3 & & \partial_2 f_3 & 1 + \partial_3 f_3 \end{pmatrix} = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Assume that $\mathbb{Z}$ embeds into R. Then this implies that $f_1 \in R[\![t_2, t_3]\!] \subseteq R[\![\boldsymbol{t}]\!]$, $f_2 \in R[\![t_3]\!] \subseteq R[\![\boldsymbol{t}]\!]$ and $f_3 = 0$. So $\boldsymbol{f}$ may be written as

$$\begin{pmatrix} t_1 + f_1(t_2, t_3) \\ t_2 + f_2(t_3) \\ t_3 \end{pmatrix}$$

and the substitution operation with an other n-tuple $\boldsymbol{g} = (t_i + g_i)_{i=1}^n$ of the same type is given by

$$\boldsymbol{g} \circ \boldsymbol{f} = \begin{pmatrix} t_1 + f_1(t_2, t_3) + g_1(t_2 + f_2(t_3), t_3) \\ t_2 + f_2(t_3) + g_2(t_3) \\ t_3 \end{pmatrix}.$$

Example 4.6. Let n equal 2. Assume $\mathbb{Z}$ embeds into R and let $\mathbb{U}_2$ be the unipotent group of 2×2 matrices. Let $\boldsymbol{f} = (t_i + f_i)_{i=1}^n$ be in $\mathcal{G}\ell_n(R)$. Then $\boldsymbol{f}$ is in the pseudo-algebraic group $\mathcal{U}_2(R)$ associated to $\mathbb{U}_2$ if and only if $\partial_1 f_1 = 0$, $\partial_1 f_2 = 0$ and $\partial_2 f_2 = 0$, that is $\boldsymbol{f}$ is of the form

$$\begin{pmatrix} t_1 + f_1(t_2) \\ t_2 \end{pmatrix}$$

where f_1 is any formal power series in $\mathcal{M}_1(R)$. The group product with an other element $(t_i + g_i)_{i=1}^n$ in $\mathcal{U}_2(R)$ — $g_2 = 0$ and $g_1 \in R[\![t_2]\!]$ — is given by

$$\boldsymbol{g} \circ \boldsymbol{f} = \begin{pmatrix} t_1 + f_1(t_2) + g_1(t_2) \\ t_2 \end{pmatrix}$$

It follows that $\mathcal{U}_2(R)$ is isomorphic to $(\mathcal{M}_1(R), +)$.

Example 4.7. Let $\mathbb{1}_n$ be the trivial subgroup of GL_n. If $\mathbb{Z}$ embeds into R, then the associated pseudo-algebraic subgroup is the trivial subgroup $\mathcal{1}_n(R)$ of $\mathcal{G}\ell_n(R)$. Conversely, if K is a finite field of characteristic p, the associated pseudo-algebraic subgroup is $\mathcal{1}_n(R) = \{\boldsymbol{t} + \boldsymbol{f}^p \mid \boldsymbol{f} \in \mathcal{M}_n^1(R)\}$.

Proposition 4.5. *Let $\mathbb{G}$ be a linear algebraic subgroup of GL_n and let $\mathcal{G}(R)$ be the associated pseudo-algebraic subgroup. Then*

$$\mathcal{G}(R) \cong \mathbb{G}(R) \ltimes \left(\mathcal{G}\ell_n^1(R) \cap \mathcal{G}(R)\right)$$

Proof. The proof is done precisely in the same way we proved Proposition 1.14. Consider the surjection $\mathcal{G}\ell_n(R) \to \mathrm{GL}_n(R)$ given in the exact sequence (1.5). Then the image of $\mathcal{G}(R)$ through such a map is contained in $\mathbb{G}(R)$, but we may also easily check that the section of the exact sequence brings $\mathbb{G}(R)$ to $\mathcal{G}(R)$. We conclude observing that the kernel of the above mentioned surjection is $\mathcal{G}\ell_n^1(R) \cap \mathcal{G}(R)$. □

4.3 Functoriality of pseudo-algebraic groups

Let R and S be K-algebras and let $\rho : R \to S$ be a K-algebra homomorphism. The universal property of the ring of formal power series [7, Chapter IV, §4, Proposition 4] implies there exists a unique ring homomorphism $\tilde{\rho} : R[\![\boldsymbol{t}]\!] \to S[\![\boldsymbol{t}]\!]$ mapping $t_i \in R[\![\boldsymbol{t}]\!]$ to $t_i \in S[\![\boldsymbol{t}]\!]$ and such that the following diagram commutes

$$\begin{tikzcd}
R \arrow[r, "\rho"] \arrow[d] & S \arrow[d] \\
R[\![\boldsymbol{t}]\!] \arrow[r, dashed, "\tilde{\rho}"] & S[\![\boldsymbol{t}]\!]
\end{tikzcd}$$

for ρ makes S (and therefore $S[\![\boldsymbol{t}]\!]$) into an R-algebra. Such homomorphism $\tilde{\rho}$ is namely the one that maps $\sum_{\boldsymbol{\alpha}\in\mathbb{N}_0{}^n} f_{\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\alpha}}$ to $\sum_{\boldsymbol{\alpha}\in\mathbb{N}_0{}^n} \rho(f_{\boldsymbol{\alpha}})\boldsymbol{t}^{\boldsymbol{\alpha}}$. Let ϕ be an endomorphism in $\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$. Then there exists a unique endomorphism $\tilde{\tilde{\rho}}(\phi)$ of $S[\![\boldsymbol{t}]\!]$ such that the following diagram commutes

$$\begin{tikzcd}
R[\![\boldsymbol{t}]\!] \arrow[rrr, "\tilde{\rho}"] \arrow[dd, "\phi"'] & & & S[\![\boldsymbol{t}]\!] \arrow[dd, dashed, "\tilde{\tilde{\rho}}(\phi)"] \\
& R \arrow[r, "\rho"] \arrow[ul] \arrow[dl] & S \arrow[ur] \arrow[dr] & \\
R[\![\boldsymbol{t}]\!] \arrow[rrr, "\tilde{\rho}"] & & & S[\![\boldsymbol{t}]\!]
\end{tikzcd}$$

namely the unique endomorphism $S[\![\boldsymbol{t}]\!] \to S[\![\boldsymbol{t}]\!]$ such that

$$\begin{tikzcd}
R[\![\boldsymbol{t}]\!] \arrow[r, "\tilde{\rho}"] & S[\![\boldsymbol{t}]\!] \arrow[dd, dashed, "\tilde{\tilde{\rho}}(\phi)"] & \\
\{t_1, \ldots, t_n\} \arrow[u] \arrow[d] & & S \arrow[ul] \arrow[dl] \\
R[\![\boldsymbol{t}]\!] \arrow[r, "\tilde{\rho}\phi"] & S[\![\boldsymbol{t}]\!] &
\end{tikzcd}$$

i. e. the one that maps $\sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\alpha}}$ to $\sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}}\tilde{\rho}(\phi(\boldsymbol{t}^{\alpha}))$. Because of uniqueness, standard arguments show that $\tilde{\tilde{\rho}}$ is a monoid morphism and in particular a group morphism when restricted to $\mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$. Of course such a monoid (group) homomorphism induces a monoid (group) homomorphism $\mathcal{M}_n(R) \to \mathcal{M}_n(S)$ (resp. $\mathcal{G}\ell_n(R) \to \mathcal{G}\ell_n(S)$) — namely the one mapping $\boldsymbol{f} = (f_i)_{i=1}^n \in \mathcal{M}_n(R)$ to $(\tilde{\rho}(f_i))_{i=1}^n$ — that we also denote $\tilde{\tilde{\rho}}$. Note that if ρ is continuous, so it is $\tilde{\rho}$, since it acts component-wise like ρ and on $\mathcal{M}_n(R)$ we have the product topology.

Now, let $f = \sum_{\boldsymbol{\alpha}\in\mathbb{N}_0{}^n} f_{\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\alpha}}$ be in $R[\![\boldsymbol{t}]\!]$ and $D = \sum_{i=1}^n D_i\partial_i \in \mathrm{Der}_R(R[\![\boldsymbol{t}]\!])$ a derivation (see Chapter 2). Then we have

$$\tilde{\rho}(Df) = \sum_{i=1}^{n} \tilde{\rho}(D_i)\tilde{\rho}(\partial_i f)$$

where

$$\tilde{\rho}(\partial_i f) = \sum_{\boldsymbol{\alpha}\in\mathbb{N}_0{}^n} \rho(f_{\boldsymbol{\alpha}})\alpha_i \boldsymbol{t}^{\boldsymbol{\alpha}-\boldsymbol{\epsilon}_i} = \partial_i(\tilde{\rho}(f))$$

and therefore, for every $\boldsymbol{f} = (f_i)_{i=1}^n \in \mathcal{M}_n(R)$,

$$\tilde{\rho}(\mathrm{Jac}\boldsymbol{f}) = (\tilde{\rho}(\partial_j f_i))_{i,j=1}^n = (\partial_j \tilde{\rho}(f_i))_{i,j=1}^n = \mathrm{Jac}(\tilde{\tilde{\rho}}(\boldsymbol{f})).$$

It follows that if $\mathrm{Jac}(\boldsymbol{f})$ satisfies some polynomial $p \in K[X_{1,1}, \ldots, X_{n,n}]$, so it does $\mathrm{Jac}(\tilde{\tilde{\rho}}(\boldsymbol{f}))$. For any algebraic group $\mathbb{G}$, let $\mathcal{G}(R)$ and $\mathcal{G}(S)$ be its associated pseudo-algebraic groups in $\mathcal{G}\ell_n(R)$

and $\mathcal{G}\ell_n(S)$ respectively. Then, from previous considerations, we infer that the restriction of $\tilde{\tilde{\rho}}$ to $\mathcal{G}(R)$ actually goes to $\mathcal{G}(S)$.

Let $\sigma : S \to T$ be a K-algebra homomorphism and let $\tilde{\tilde{\sigma}}$ be the associated group morphism from $\mathcal{G}\ell_n(S)$ to $\mathcal{G}\ell_n(T)$. Then, for every $\boldsymbol{f} = (\sum_{\boldsymbol{\alpha}\in{\mathbb{N}_0}^n} f_{i,\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\alpha}})_{i=1}^n \in \mathcal{M}_n(R)$

$$\tilde{\tilde{\sigma}}\tilde{\tilde{\rho}}(\boldsymbol{f}) = \tilde{\tilde{\sigma}}(\tilde{\tilde{\rho}}(f)) = \tilde{\tilde{\sigma}}\left(\left(\sum_{\boldsymbol{\alpha}} \rho(f_{i,\boldsymbol{\alpha}})\boldsymbol{t}^{\boldsymbol{\alpha}}\right)_{i=1}^n\right) = \left(\sum_{\boldsymbol{\alpha}} \sigma\rho(f_{i,\boldsymbol{\alpha}}))\boldsymbol{t}^{\boldsymbol{\alpha}}\right)_{i=1}^n = \widetilde{\widetilde{\sigma\rho}}(\boldsymbol{f})$$

where $\widetilde{\widetilde{\sigma\rho}}$ is the monoid homomorphism $\mathcal{M}_n(R) \to \mathcal{M}_n(T)$ associated to $\sigma\rho : R \to T$. Finally, clearly the group homomorphism associated to $\mathrm{id}_R : R \to R$ is $\tilde{\tilde{\mathrm{id}}}_R = \mathrm{id}_{\mathcal{M}_n(R)}$. All these considerations sum up by saying that for every linear algebraic embedding $\mathbb{G} \hookrightarrow \mathrm{GL}_n$ over K we have an associated functor $\mathcal{G}$, called pseudo-algebraic functor, from the category of (topological) K-algebras to the category of (topological) groups.

Lemma 4.6. *Let $\rho : R \to S$ be an injective K-algebras morphism. Then the induced map $\tilde{\tilde{\rho}} : \mathcal{G}\ell_n(R) \to \mathcal{G}\ell_n(S)$ is injective.*

Proof. Let $\boldsymbol{f} = (\sum_{\boldsymbol{\alpha}} f_{i,\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\alpha}})_{i=1}^n$ and $\boldsymbol{g} = (\sum_{\boldsymbol{\alpha}} g_{i,\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\alpha}})_{i=1}^n$ be two elements of $\mathcal{G}\ell_n(R)$ such that $\tilde{\tilde{\rho}}(\boldsymbol{f}) = \tilde{\tilde{\rho}}(\boldsymbol{g})$. Using the explicit expression of $\tilde{\tilde{\rho}}$, we have

$$\tilde{\tilde{\rho}}(\boldsymbol{f}) = \left(\sum_{\boldsymbol{\alpha}} \rho(f_{i,\boldsymbol{\alpha}})\boldsymbol{t}^{\boldsymbol{\alpha}}\right)_{i=1}^n = \left(\sum_{\boldsymbol{\alpha}} \rho(g_{i,\boldsymbol{\alpha}})\boldsymbol{t}^{\boldsymbol{\alpha}}\right)_{i=1}^n = \tilde{\tilde{\rho}}(\boldsymbol{g})$$

that holds only if

$$\rho(f_{i,\boldsymbol{\alpha}}) = \rho(g_{j,\boldsymbol{\alpha}})$$

for every $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$ and every $i \in \{1, \dots, n\}$, that is $\boldsymbol{f} = \boldsymbol{g}$, since ρ is injective. □

Remark 4.7. The functor $\mathcal{G}$ does not preserve surjectivity in general. For example, let K and R be the ring of integers $\mathbb{Z}$ and consider the surjective ring morphism $\rho : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$ where p is a prime number. Then the induced morphism $\mathrm{GL}_n(\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ is not necessarily surjective. For example, when $p = 7$ and $n = 2$, the matrix

$$\begin{pmatrix} 2 + 7\mathbb{Z} & 0 \\ 0 & 2 + 7\mathbb{Z} \end{pmatrix}$$

is in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ but not in the image of $\mathrm{GL}_2(\mathbb{Z})$, thus $\tilde{\tilde{\rho}} : \mathcal{G}\ell_2(\mathbb{Z}) \to \mathcal{G}\ell_2(\mathbb{Z}/7\mathbb{Z})$ cannot be surjective. However its restriction to $\mathcal{G}\ell_n^1(\mathbb{Z})$ it is, but somewhat by chance. A simple counterexample is given by the trivial pseudo-algebraic subgroup, discussed in Example 4.7. Indeed $\mathit{1}_n(\mathbb{Z})$ is actually trivial, whereas $\mathit{1}_n(\mathbb{Z}/p\mathbb{Z})$ is not, so the induced map $\mathit{1}_n(\mathbb{Z}) \to \mathit{1}_n(\mathbb{Z}/p\mathbb{Z})$ can not be surjective, not even when restricted to the intersection with the Nottingham group.

Lemma 4.8. *Let I be a closed ideal of R. Then the subset*

$$\left\{\boldsymbol{f} = (t_i + \sum_{\boldsymbol{\alpha}} f_{i,\boldsymbol{\alpha}})_{i=1}^n \in \mathcal{G}\ell_n(R) \mid f_{i,\boldsymbol{\alpha}} \in I \text{ for every } i \in \{1, \dots, n\},\ \boldsymbol{\alpha} \in {\mathbb{N}_0}^n\right\}$$

is a normal closed subgroup of $\mathcal{G}\ell_n(R)$.

Proof. Such a subset is the kernel of the map $\mathcal{G}\ell_n(R) \to \mathcal{G}\ell_n(R/I)$. □

4.4 Lie rings of pseudo-algebraic groups

Let $\mathcal{G}$ be a pseudo-algebraic functor over K. Coherently with [41, Theorem 12.2], we define

$$\operatorname{Lie}(\mathcal{G})(R) := \ker\left(\mathcal{G}\left(R[\tau]/(\tau^2)\right) \to \mathcal{G}(R)\right).$$

Since $\mathcal{G}\left(R[\tau]/\tau^2\right)$ and $\mathcal{G}(R)$ are closed subgroups of $\mathcal{Gl}_n\left(R[\tau]/\tau^2\right)$ and $\mathcal{Gl}_n(R)$ respectively and the projection $\mathcal{G}\left(R[\tau]/\tau^2\right) \to \mathcal{G}(R)$ is just the restriction to $\mathcal{G}\left(R[\tau]/\tau^2\right)$ of the projection from $\mathcal{Gl}_n\left(R[\tau]/\tau^2\right)$ to $\mathcal{Gl}_n(R)$, there exists a natural embedding of $\operatorname{Lie}(\mathcal{G})(R)$ into $\operatorname{Lie}(\mathcal{Gl}_n)(R)$.

Notation 17. We write $R[\tau]$ — assuming $\tau^2 = 0$ — instead of $R[\tau]/(\tau^2)$.

Let S be a K-algebra such that there exists an embedding $R[\tau] \to S$. Then, because of functoriality of pseudo-algebraic groups, we have an embedding of $\operatorname{Lie}(\mathcal{G})(R)$ into $\mathcal{G}(S)$. Let $\boldsymbol{f} = \boldsymbol{t} + \tau\boldsymbol{f}'$ — for some $\boldsymbol{f}' = (f_i)_{i=1}^n \in \mathcal{M}_n(R)$ — be an arbitrary element of $\operatorname{Lie}(\mathcal{G})(R) \leq \mathcal{G}(S)$. Using automorphism representation of $\mathcal{Gl}_n(S)$, we may consider $\boldsymbol{f}$ as an automorphism $\Phi_{\boldsymbol{f}}$ of $S[\![\boldsymbol{t}]\!]$ whose action is defined by $g \in S[\![\boldsymbol{t}]\!] \mapsto g \circ \boldsymbol{f}$. Then, by Lemma 1.17,

$$\Phi_{\boldsymbol{f}}(g) = g \circ \boldsymbol{f} = \sum_{\boldsymbol{\alpha}} (\tau\boldsymbol{f}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} g = g + \tau \sum_{i=1}^n f_i \partial_i g$$

that is, $\Phi_{\boldsymbol{f}}$ acts like the S-linear morphism $\mathrm{id} + \tau D$ where $D = \sum_{i=1}^n f_i \partial_i$ is in the image of $\operatorname{Der}^0_R(R[\![\boldsymbol{t}]\!])$ into $\operatorname{Der}^0_S(S[\![\boldsymbol{t}]\!])$ (see Lemma 2.3). Thus, we obtain a natural map from $\operatorname{Lie}(\mathcal{G})(R)$ to $\operatorname{Der}^0_R(R[\![\boldsymbol{t}]\!])$, that maps $\boldsymbol{f}$ to the derivation $D_{\boldsymbol{f}}$ such that $\tau D_{\boldsymbol{f}}(g) = g \circ \boldsymbol{f} - g$ for every $g \in R[\![\boldsymbol{t}]\!]$. Note that $\boldsymbol{f} = \boldsymbol{t} \circ \boldsymbol{f} = (\mathrm{id} + \tau D_{\boldsymbol{f}})\boldsymbol{t} = \boldsymbol{t} + \tau D_{\boldsymbol{f}}\boldsymbol{t}$ (the R-morphisms are meant to be appplied component-wise to n-tuples), thus the above mentioned map is injective, since there is a left inverse given by $D \in \operatorname{Der}^0_R(R[\![\boldsymbol{t}]\!]) \mapsto \boldsymbol{t} + \tau D\boldsymbol{t}$. From the explicit expression of the maps it is also clear that it is continuous.

Proposition 4.9. *The just mentioned map from* $\operatorname{Lie}(\mathcal{G})(R)$ *to* $\operatorname{Der}^0_R(R[\![\boldsymbol{t}]\!])$ *is an homomorphism of abelian groups.*

Proof. Let $\boldsymbol{f} = \boldsymbol{t} + \tau\boldsymbol{f}'$ and $\boldsymbol{g} = \boldsymbol{t} + \tau\boldsymbol{g}'$ be two elements of $\operatorname{Lie}(\mathcal{G})(R)$. Then, using Lemma 1.17

$$(\boldsymbol{t} + \tau\boldsymbol{f}') \circ (\boldsymbol{t} + \tau\boldsymbol{g}') = \boldsymbol{t} + \tau\boldsymbol{g}' + \tau\boldsymbol{f}' \circ (\boldsymbol{t} + \tau\boldsymbol{g}') = \boldsymbol{t} + \tau(\boldsymbol{g}' + \boldsymbol{f}')$$

so that the image of $\boldsymbol{f} \circ \boldsymbol{g}$ in $\operatorname{Der}^0_R(R[\![\boldsymbol{t}]\!])$ is

$$\sum_{i=1}^n (f_i + g_i)\partial_i = \sum_{i=1}^n f_i\partial_i + \sum_{i=1}^n g_i\partial_i = D_{\boldsymbol{f}} + D_{\boldsymbol{g}}$$

where $\boldsymbol{f}' = (f_i)_{i=1}^n$, $\boldsymbol{g}' = (g_i)_{i=1}^n$ and $D_{\boldsymbol{f}}$ and $D_{\boldsymbol{g}}$ are the images into $\operatorname{Der}^0_R(R[\![\boldsymbol{t}]\!])$ of $\boldsymbol{f}$ and $\boldsymbol{g}$ respectively. □

Consider $R[\mu, \eta]/(\mu^2, \eta^2)$, simply denoted by $R[\mu, \eta]$. Then we have three embedding κ_μ, κ_η, $\kappa_{\mu\eta}$ of $\operatorname{Lie}(\mathcal{G})(R)$ into $\mathcal{G}(S)$, sending τ to μ, η or $\mu\eta$, respectively. Consider two elements $\boldsymbol{f} = \boldsymbol{t} + \tau\boldsymbol{f}'$ and $\boldsymbol{g} = \boldsymbol{t} + \tau\boldsymbol{g}'$ in $\operatorname{Lie}(\mathcal{G})(R)$ and let $D_{\boldsymbol{f}}$ and $D_{\boldsymbol{g}}$ be their associated derivations. Then $\kappa_\mu(\boldsymbol{f})$ acts like $\mathrm{id} + \mu D_{\boldsymbol{f}}$, its inverse like $\mathrm{id} - \mu D_{\boldsymbol{f}}$ and similarly for $\kappa_\eta(\boldsymbol{g})$. Thus, for every formal power series $h \in R[\![\boldsymbol{t}]\!]$

$$\begin{aligned} h \circ [\kappa_\mu(\boldsymbol{f}), \kappa_\eta(\boldsymbol{g})] =& h \circ (\boldsymbol{t} - \mu \boldsymbol{f}') \circ (\boldsymbol{t} - \eta \boldsymbol{g}') \circ (\boldsymbol{t} + \mu \boldsymbol{f}') \circ (\boldsymbol{t} + \eta \boldsymbol{g}') \\ =& (\mathrm{id} + \eta D_{\boldsymbol{g}})(\mathrm{id} + \mu D_{\boldsymbol{f}})(\mathrm{id} - \eta D_{\boldsymbol{g}})(\mathrm{id} - \mu D_{\boldsymbol{f}})h \\ =& (\mathrm{id} + \eta D_{\boldsymbol{g}})(\mathrm{id} + \mu D_{\boldsymbol{f}})(\mathrm{id} - \eta D_{\boldsymbol{g}})(h - \mu D_{\boldsymbol{f}} h) \\ =& (\mathrm{id} + \eta D_{\boldsymbol{g}})(\mathrm{id} + \mu D_{\boldsymbol{f}})(h - \mu D_{\boldsymbol{f}} h - \eta D_{\boldsymbol{g}} h + \eta\mu D_{\boldsymbol{g}} D_{\boldsymbol{f}} h) \\ =& (\mathrm{id} + \eta D_{\boldsymbol{g}})(h - \mu D_{\boldsymbol{f}} h - \eta D_{\boldsymbol{g}} h + \eta\mu D_{\boldsymbol{g}} D_{\boldsymbol{f}} h + \mu D_{\boldsymbol{f}} h - \mu\eta D_{\boldsymbol{f}} D_{\boldsymbol{g}} h) \\ =& h - \eta D_{\boldsymbol{g}} h + \eta\mu \left(D_{\boldsymbol{g}} D_{\boldsymbol{f}} - D_{\boldsymbol{f}} D_{\boldsymbol{g}}\right) h + \eta D_{\boldsymbol{g}} h - \eta\mu D_{\boldsymbol{g}} D_{\boldsymbol{f}} h + \eta\mu D_{\boldsymbol{g}} D_{\boldsymbol{f}} h \\ =& \left(\mathrm{id} + \eta\mu \left[D_{\boldsymbol{g}}, D_{\boldsymbol{f}}\right]\right) h; \end{aligned}$$

therefore $[\kappa_\mu(\boldsymbol{f}), \kappa_\eta(\boldsymbol{g})] \in \mathcal{G}\left(R[\mu, \eta]\right)$ is in the image of $\kappa_{\mu,\eta}$, that is there exists $\boldsymbol{h} = (\boldsymbol{t} + \tau \boldsymbol{h}')$ in $\mathrm{Lie}\left(\mathcal{G}\right)(R)$ such that the associated derivation is $[D_{\boldsymbol{g}}, D_{\boldsymbol{f}}]$. It follows that the image of $\mathrm{Lie}\left(\mathcal{G}\right)(R)$ into $\mathrm{Der}^0_R\left(R[\![\boldsymbol{t}]\!]\right)$ is a Lie subring, or — equivalently — we may endow $\mathrm{Lie}\left(\mathcal{G}\right)(R)$ of a Lie brackets operation that turns it into a Lie ring, namely $[\boldsymbol{g}, \boldsymbol{f}] := \kappa_{\mu\eta}^{-1}([\kappa_\mu(\boldsymbol{f}), \kappa_\eta(\boldsymbol{g})])$.

Remark 4.10. The order in the definition of Lie brackets in $\mathrm{Lie}\left(\mathcal{G}\right)(R)$ is inverted so that the resulting Lie ring is isomorphic (and not *anti*-isomorphic) as a Lie ring to its image in $\mathrm{Der}^0_R\left(R[\![\boldsymbol{t}]\!]\right)$.

Example 4.8. The Lie ring of $\mathcal{Gl}_n\left(R\right)$ is isomorphic to $\mathrm{Der}^0_R\left(R[\![\boldsymbol{t}]\!]\right)$. In fact, for every derivation D in $\mathrm{Der}^0_R\left(R[\![\boldsymbol{t}]\!]\right)$, the element given by $\boldsymbol{t} + \tau D\boldsymbol{t}$ is in $\mathcal{M}_n\left(R[\tau]\right)$ and it is invertible, its inverse being $\boldsymbol{t} - \tau D\boldsymbol{t}$.

Example 4.9. Let $\boldsymbol{f} = (t_i + \tau f_i)_{i=1}^n$ be in $\mathrm{Lie}\left(\mathcal{Gl}_n\right)(R)$. Then the computation of the determinant of $\mathrm{Jac}(\boldsymbol{f})$ reduces to $1 + \tau \sum_{i=1}^n \partial_i f_i$, since in all other terms τ^2 appears. So $\mathrm{Lie}\left(\mathcal{Sl}_n\right)(R)$ coincides with the subset of $\mathrm{Der}^0_R\left(R[\![\boldsymbol{t}]\!]\right)$ of derivations $\sum_{i=1}^n f_i \partial_i$ such that $\sum_{i=1}^n \partial_i f_i = 0$, that is the intersection of the special algebra (see Chapter 3) and $\mathrm{Der}^0_R\left(R[\![\boldsymbol{t}]\!]\right)$.

Chapter 5

Other families of subgroups of the generalized Nottingham group

In this section we assume R to be a finite dimensional algebra over a p prime order field. Actually, the reader may verify that for the first section to work it is enough requiring R to be Noetherian, whereas most of the second section may be done with arbitrary rings. Still, for the sake of homogeneity and to avoid specifying each time what we are dealing with, we preferred having this general assumption.

5.1 Subgroups related to ideals

We have already introduced subgroups of $\mathcal{Gl}_n(R)$ associated to ideals of R (Lemma 4.8). Here we construct subgroups starting from ideals of $R[\![\boldsymbol{t}]\!]$.

Lemma 5.1. *Let I be an ideal of $R[\![\boldsymbol{t}]\!]$ and let ϕ be an automorphism of $R[\![\boldsymbol{t}]\!]$ such that $\phi(I) \subseteq I$. Then $\phi(I) = I$.*

Proof. Since $R[\![\boldsymbol{t}]\!]$ is Noetherian [12] the sequence $I \subseteq \phi(I) \subseteq \phi^2(I) \subseteq \ldots$ stabilizes, that is $\phi^i(I) = \phi^{i+1}(I)$ for some $i \in \mathbb{N}$ and therefore we obtain $\phi(I) = I$ by applying ϕ^{-r}. □

Proposition 5.2. *Let I be a closed ideal of $R[\![\boldsymbol{t}]\!]$. Then*

$$\mathcal{St}(I) := \{\boldsymbol{g} \in \mathcal{Gl}_n(R) \mid h \circ \boldsymbol{g} \in I \text{ for every } h \in I\}$$

and

$$\mathcal{K}(I) := \{(t_i + f_i)_{i=1}^n \in \mathcal{Gl}_n(R) \mid f_i \in I\}$$

are closed subgroups of $\mathcal{Gl}_n(R)$.

Proof. Identifying $\mathcal{Gl}_n(R)$ with $\mathrm{Aut}_R R[\![\boldsymbol{t}]\!]$, the set $\mathcal{St}(I)$ coincides with the set of automorphisms ϕ such that $\phi(I) \subseteq I$, that, by the previous lemma, coincides with the set of automorphisms such that $\phi(I) = I$, that is a group, being a stabilizer of the action of the group on ideals of $R[\![\boldsymbol{t}]\!]$.

Let $\boldsymbol{f}$ be in $\mathcal{Gl}_n(R) \setminus \mathcal{St}(I)$. Then there exists $i \in I$ such that $i \circ \boldsymbol{f} \notin I$. Since I is closed, there exists an open neighbourhood of $i \circ \boldsymbol{f}$ in $\mathfrak{m}$ such that $I \cap O = \emptyset$. By Corollary 1.28, the subset $\{\boldsymbol{g} \in \mathcal{M}_n(R) \mid i \circ \boldsymbol{g} \in O\}$ is an open neighbourhood of $\boldsymbol{f}$ that does not meet $\mathcal{St}(I)$. So $\mathcal{St}(I)$ is closed.

On the group $\mathcal{S}t\,(I)$ we can define a continuous group morphism $\mathcal{S}t\,(I) \to \mathrm{Aut}_R(R[\![\boldsymbol{t}]\!]/I)$ such that every $\boldsymbol{f} \in \mathcal{S}t\,(I)$ is mapped to the automorphism $f + I \mapsto f \circ \boldsymbol{f} + I$. The kernel of such a morphism is $\mathcal{K}\,(I)$ that therefore is a normal closed subgroup of $\mathcal{S}t\,(I)$. □

Example 5.1. When $I = \mathfrak{m}^j$ for some $j \in \mathbb{N}$, we have that the group $\mathcal{S}t\left(\mathfrak{m}^j\right)$ is the whole group $\mathcal{G}\ell_n\,(R)$, while $\mathcal{K}\left(\mathfrak{m}^j\right)$ equals $\mathcal{G}\ell_n^{j-1}\,(R)$.

Proposition 5.3. *Let I and J be ideals of $R[\![\boldsymbol{t}]\!]$. Then*

(i) $\mathcal{K}\,(I)$ is open if and only if I is open;

(ii) $\mathcal{S}t\,(I) \cap \mathcal{S}t\,(J) \subseteq \mathcal{S}t\,(I \cap J)$ and $\mathcal{K}\,(I) \cap \mathcal{K}\,(J) = \mathcal{K}\,(I \cap J)$;

(iii) the subgroup generated by $\mathcal{K}\,(I)$ and $\mathcal{K}\,(J)$ is contained in $\mathcal{K}\,(I+J)$;

(iv) the closed subgroup generated by $\mathcal{K}\,(J) \cap \mathcal{G}\ell_n^1\,(R)$ and $\mathcal{K}\,(I) \cap \mathcal{G}\ell_n^1\,(R)$ is $\mathcal{K}\,(I+J) \cap \mathcal{G}\ell_n^1\,(R)$.

Proof. Proofs of (i), (ii) and (iii) follow straightforward from definitions, so we focus on (iv).

Let G denote the closed subgroup generated by $\mathcal{K}\,(I)$ and $\mathcal{K}\,(J)$ and let $\boldsymbol{f}$ be in the intersection of $\mathcal{K}\,(I+J)$ and $\mathcal{G}\ell_n^1\,(R)$. We prove by induction that for every $r \in \mathbb{N}$ there exists $\boldsymbol{h}_r \in G$ such that $\boldsymbol{f} \circ \boldsymbol{h}_r$ is in $\mathcal{G}\ell_n^r\,(R)$. Since G is closed, this implies that the coset of G with respect to $\boldsymbol{f}$ contains the identity, i. e. $\boldsymbol{f}$ is in G.

For $r = 1$ it is trivial. Assume it holds for some $r \in \mathbb{N}$. Then $\boldsymbol{f}_r := (\boldsymbol{t} + \boldsymbol{f}) \circ \boldsymbol{h}_r$ is in $\mathcal{G}\ell_n^r\,(R) \cap \mathcal{K}\,(I+J)$. By definition of $\mathcal{K}\,(I+J)$, it means that there exist $\boldsymbol{f}_I \in \bigoplus_{i=1}^n I \subseteq (R[\![\boldsymbol{t}]\!])^n$ and $\boldsymbol{f}_J \in \bigoplus_{i=1}^n I \subseteq (R[\![\boldsymbol{t}]\!])^n$, both of order at least $r+1$, such that $\boldsymbol{f}_r = \boldsymbol{t} + \boldsymbol{f}_I + \boldsymbol{f}_J$. So let $\boldsymbol{h}_{r+1}$ be $\boldsymbol{h}_r \circ (\boldsymbol{t} - \boldsymbol{f}_I) \circ (\boldsymbol{t} - \boldsymbol{f}_J)$, that is in G. By formula (1.8), we have

$$\boldsymbol{f} \circ \boldsymbol{h}_{r+1} = \boldsymbol{f}_r \circ (\boldsymbol{t} - \boldsymbol{f}_I) \circ (\boldsymbol{t} - \boldsymbol{f}_J) \equiv \boldsymbol{t} \mod \mathcal{M}_n^{r+2}(R)$$

i. e. $\boldsymbol{f} \circ \boldsymbol{h}_{r+1}$ is in $\mathcal{G}\ell_n^{r+1}\,(R)$. □

Example 5.2. Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_r$ be in $\mathbb{N}_0{}^n$ and for every $i \in \{1, \ldots, r\}$ let $(\boldsymbol{t}^{\boldsymbol{\alpha}_i})$ denote the closed ideal of $R[\![\boldsymbol{t}]\!]$ generated by $\boldsymbol{t}^{\boldsymbol{\alpha}_i}$. Then, if n is at least 2, every $\mathcal{K}\,((\boldsymbol{t}^{\boldsymbol{\alpha}_j}))$ is not open for any $j = 1, \ldots r$. Assume that $(\boldsymbol{t}^{\boldsymbol{\alpha}_1}) + \ldots + (\boldsymbol{t}^{\boldsymbol{\alpha}_r})$ is open. Then any closed subgroup of $\mathcal{G}\ell_n\,(R)$ that contains $\mathcal{K}\,((\boldsymbol{t}^{\boldsymbol{\alpha}_1})), \ldots, \mathcal{K}\,((\boldsymbol{t}^{\boldsymbol{\alpha}_r}))$ is open, since it contains $\mathcal{K}\,((\boldsymbol{t}^{\boldsymbol{\alpha}_1}) + \ldots + (\boldsymbol{t}^{\boldsymbol{\alpha}_r})) \cap \mathcal{G}\ell_n^1\,(R)$. This happens if and only if for every $i \in \{1, \ldots, n\}$ there is $j \in \{1, \ldots, r\}$ such that $\boldsymbol{\alpha}_j = {t_i}^{x_i}$ for some $x_i \in \mathbb{N}$.

Example 5.3. Let R be the finite field $\mathbb{F}_p$ for a prime p. Consider the (open) ideal $I \trianglelefteq R[\![\boldsymbol{t}]\!]$ generated by $t_1^p, \ldots, t_n^p$. For every $\boldsymbol{f} = (f_j)_{j=1}^n \in \mathcal{G}\ell_n\,(\mathbb{F}_p)$ and every $i \in \{1, \ldots, n\}$, the automorphism associated to $\boldsymbol{f}$ applied to ${t_i}^p$ gives ${f_i}^p$ that is in I. Thus $\mathcal{S}t\,(I)$ is the whole group $\mathcal{G}\ell_n\,(\mathbb{F}_p)$ and therefore $\mathcal{K}\,(I)$ is an open normal subgroup of $\mathcal{G}\ell_n\,(\mathbb{F}_p)$ and in particular of $\mathcal{G}\ell_n^1\,(\mathbb{F}_p)$. By Proposition 2.7, its associated Lie subalgebra $L_{\mathcal{G}\ell_n^1(\mathbb{F}_p)}(\mathcal{K}\,(I))$ is an open ideal of $L(\mathcal{G}\ell_n^i\,(\mathbb{F}_p)) \cong \mathrm{Der}^1_{\mathbb{F}_p}\,(\mathbb{F}_p[\![\boldsymbol{t}]\!])$, namely $\{\sum_{i=1}^n f_i \partial_i \mid f_i \in I\}$. It turns out that the quotient algebra $L(\mathcal{G}\ell_n^i\,(\mathbb{F}_p))/L_{\mathcal{G}\ell_n^1(\mathbb{F}_p)}(\mathcal{K}\,(I))$ is isomorphic to $\mathrm{Der}_{\mathbb{F}_p}\,(\mathbb{F}_p[t_1, \ldots, t_n]/({t_1}^p, \ldots, {t_n}^p))$ that in turn is isomorphic to a subalgebra of the n-th Witt algebra $W(n : \boldsymbol{1})$. This enforces the relation discussed in the introduction of Chapter 3 between the Nottingham group over finite fields and Witt algebras.

5.2 Index-subgroups

Index-subgroups are subgroups of the Nottingham introduced by Barnea and Klopsch [3]. Some of them are part of the family — mentioned in the introduction of this thesis — of closed subgroups of the Nottingham group that are hereditarily just infinite. However, their importance is maybe more related to the computation of the Hausdorff spectrum of the Nottingham group (see Theorem 5.15).

In this section, imitating Barnea and Klopsch, we present analogous of index subgroups for the generalized Nottingham group over a finite dimensional algebra R over the finite field $\mathbb{F}_p$ of order a prime p.

We have already defined in Chapter 1 (Section 1.1.1) what the support of a formal power series is. Here we recall it and — with an abuse of notation — we extend this concept to elements of $\mathcal{G}\ell^1_n(R)$.

Definition. For every formal power series $f = \sum_{\boldsymbol{\alpha}} f_{\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}}$ in $R[\![\boldsymbol{t}]\!]$, the support of f is the set $\mathrm{Supp} f$ of n-tuples $\boldsymbol{\alpha}$ in ${\mathbb{N}_0}^n$ such that $f_{\boldsymbol{\alpha}}$ is not $0 \in R$.

Definition. Let $\boldsymbol{f} = (t_i + f_i)_{i=1}^n$ be an element of $\mathcal{G}\ell^1_n(R)$. We define its support to be the subset of ${\mathbb{N}_0}^n \times \{1, \dots, n\}$ given by

$$\mathrm{Supp}\boldsymbol{f} := \bigcup_{i=1}^{n} \mathrm{Supp} f_i \times \{i\} \subseteq {\mathbb{N}_0}^n \times \{1, \dots, n\}. \tag{5.1}$$

Moreover, for every $d \in \mathbb{N}$ we define the restricted d-support of $\boldsymbol{f}$ to be

$$\mathrm{Supp}_d \boldsymbol{f} := \{(\boldsymbol{\alpha}, i) \in \mathrm{Supp}\boldsymbol{f} \mid |\boldsymbol{\alpha}| \le \omega(\boldsymbol{f}) + d\}. \tag{5.2}$$

The concept of support of an element of $\mathcal{G}\ell^1_n(R)$ is fundamental in the proof of Theorem 0.2, However we have already introduced it as it is useful to give a concise definition of index-subgroup.

Definition. Let I be a subset of ${\mathbb{N}_0}^n \times \{1, \dots, n\}$ and define

$$\mathcal{I}(I) := \{\boldsymbol{t} + \boldsymbol{f} \in \mathcal{M}_n(R) \mid \mathrm{Supp}\boldsymbol{f} \subseteq I\}$$

When $\mathcal{I}(I)$ is a subgroup of $\mathcal{G}\ell^1_n(R)$, we call it index-subgroup associated to I.

Definition. We say that $I \subseteq {\mathbb{N}_0}^n \times \{1, \dots, n\}$ is an admissible index-set if for every $(\boldsymbol{\alpha}, i)$ in I the weight of $\boldsymbol{\alpha}$ is greater than 1 and for all $(\boldsymbol{\alpha}, i)$, $(\boldsymbol{\beta}, j)$ in I and for every $h \in \mathbb{N}$ such that $\binom{\boldsymbol{\beta}}{h\boldsymbol{\epsilon}_j} \not\equiv_p 0$, the pair $(h\boldsymbol{\alpha} + \boldsymbol{\beta} - h\boldsymbol{\epsilon}_i, j)$ is in I.

Notation 18. The requirement $|\boldsymbol{\alpha}| > 1$ for every $(\boldsymbol{\alpha}, i) \in I$ for I to be admissible is trivially needed for $\mathcal{I}(I)$ to be a subset of $\mathcal{G}\ell^1_n(R)$. From now on it is implicit, i. e. whenever we consider a subset I of ${\mathbb{N}_0}^n \times \{1, \dots, n\}$, we assume that any $(\boldsymbol{\alpha}, i)$ is in I only if $|\boldsymbol{\alpha}| > 1$.

Remark 5.4. There is a natural injection of ${\mathbb{N}_0}^n \times \{1, \dots, n\}$ into ${\mathbb{N}_0}^{n+1} \times \{1, \dots, n+1\}$, namely $((\alpha_1, \dots, \alpha_n), i) \mapsto ((\alpha_1, \dots, \alpha_n, 0), i)$. If $I \subseteq {\mathbb{N}_0}^n \times \{1, \dots, n\}$ is an admissible index-set, then its image in ${\mathbb{N}_0}^{n+1} \times \{1, \dots, n+1\}$ is trivially again an admissible set (for $n + 1$).

Lemma 5.5. *Let I be an admissible index-set. Then the set $\mathcal{I}(I)$ coincides with the closed sub-semigroup of $\mathcal{G}\ell^1_n(R)$ topologically generated by $S := \{\boldsymbol{t} + a\boldsymbol{t}^{\boldsymbol{\alpha}}\boldsymbol{E}_i \mid (\boldsymbol{\alpha}, i) \in I \text{ and } a \in R\}$, that, actually, is a subgroup.*

Proof. Clearly $S = \{a\boldsymbol{t}^{\boldsymbol{\alpha}}\boldsymbol{E}_i \in \mathscr{G}\ell^1_n(R) \mid (\boldsymbol{\alpha}, i) \in I \text{ and } a \in R\}$ is contained in $\mathscr{I}(I)$ and one can also easily check that $\mathscr{I}(I)$ is a closed set (roughly speaking, it is homeomorphic to $\prod_{(\boldsymbol{\alpha},i)\in I} R \times \prod_{(\boldsymbol{\alpha},i)\notin I}\{0\}$, when looking at $\mathscr{M}_n(R) \supseteq \mathscr{G}\ell^1_n(R)$ as an infinite product of R with itself). Thus it is enough to show that for every $\boldsymbol{t}+\boldsymbol{f} \in \mathscr{I}(I)$ and every $\boldsymbol{g}$ in the subsemigroup generated by S, the element $(\boldsymbol{t}+\boldsymbol{f})\circ\boldsymbol{g}$ is contained in $\mathscr{I}(I)$ and — for some choice of $\boldsymbol{g}$ — equals an element of depth greater than $\omega(\boldsymbol{f})$. For this implies that the sub-semigroup generated by S is contained in $\mathscr{I}(I)$ and, for every $r \in \mathbb{N}$, it contains some $\boldsymbol{t}+\boldsymbol{f}_r$ such that $(\boldsymbol{t}+\boldsymbol{f})\circ(\boldsymbol{t}+\boldsymbol{f}_r)$ is in $\mathscr{G}\ell^r_n(R)$. It follows that the inverse of $\boldsymbol{t}+\boldsymbol{f}$ is contained in the closure of the semigroup which is contained in $\mathscr{I}(I)$.

Let $\boldsymbol{t}+\boldsymbol{f}$ be an arbitrary element of $\mathscr{I}(I)$, say $\boldsymbol{f} = \sum_{(\boldsymbol{\beta},j)\in I} f_{j,\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\beta}}\boldsymbol{E}_j$, and let $(\boldsymbol{\alpha}, i)$ be in I. Then

$$(\boldsymbol{t}+\boldsymbol{f})\circ(\boldsymbol{t}+a\boldsymbol{t}^{\boldsymbol{\alpha}}\boldsymbol{E}_i) = \boldsymbol{t}+a\boldsymbol{t}^{\boldsymbol{\alpha}}\boldsymbol{E}_i+\boldsymbol{f}+\sum_{h>0}\sum_{(\boldsymbol{\beta},j)\in I}\binom{\boldsymbol{\beta}}{h\boldsymbol{\epsilon}_i} f_{j,\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\beta}+h(\boldsymbol{\alpha}-\boldsymbol{\epsilon}_i)}\boldsymbol{E}_j \tag{5.3}$$

is in $\mathscr{I}(I)$ by hypothesis, that is $(\boldsymbol{t}+\boldsymbol{f})\circ S \subseteq \mathscr{I}(I)$. In particular, let $\{(\boldsymbol{\alpha}_1, i_1), \ldots, (\boldsymbol{\alpha}_r, i_r)\}$ be the restricted 1-support $\operatorname{Supp}_1(\boldsymbol{t}+\boldsymbol{f})$ of $(\boldsymbol{t}+\boldsymbol{f})$, then

$$(\boldsymbol{t}+\boldsymbol{f})\circ(\boldsymbol{t}-f_{i_1,\boldsymbol{\alpha}_1}\boldsymbol{t}^{\boldsymbol{\alpha}_1}\boldsymbol{E}_{i_1})\circ\cdots\circ(\boldsymbol{t}-f_{i_r,\boldsymbol{\alpha}_r}\boldsymbol{t}^{\boldsymbol{\alpha}_r}\boldsymbol{E}_{i_r})$$

by formula (1.8) is an element of $\mathscr{I}(I)$ of depth greater than $\omega(\boldsymbol{f})$. □

Remark 5.6. In fact, by taking $\boldsymbol{f} = \boldsymbol{t}^{\boldsymbol{\beta}}\boldsymbol{E}_j$ for any $(\boldsymbol{\beta}, j) \in I$ in equation (5.3), we have that the previous lemma gives a characterization of admissible index-sets which, when $n = 1$, coincides with the definition given by Barnea and Klopsch [3].

Example 5.4. Let $\boldsymbol{\gamma}$ be an n-tuple in ${\mathbb{N}_0}^n$. Consider the set

$$\mathscr{V}(\boldsymbol{\gamma}) := \{(\boldsymbol{\alpha}, i) \in {\mathbb{N}_0}^n \times \{1, \ldots, n\} \mid \boldsymbol{\alpha} \not\leq \boldsymbol{\gamma}\}$$

and let $(\boldsymbol{\alpha}, i), (\boldsymbol{\beta}, j)$ be two element of it, say $\boldsymbol{\alpha} = (\alpha_l)_{l=1}^n$ and $\boldsymbol{\beta} = (\beta_l)_{l=1}^n$. Then there exist $k, l \in \{1, \ldots, n\}$ such that $\alpha_l > \gamma_l$ and $\beta_k > \gamma_k$. If either l or k is not equal to i, the inequality $h\boldsymbol{\alpha}+\boldsymbol{\beta}-h\boldsymbol{\epsilon}_i \not\leq \gamma$ trivially holds for every positive integer $h < \beta_i$. Suppose $i = l = k$. Then $h\alpha_i + \beta_i - h \geq h\alpha_i \not\leq \gamma_i$ for every $h \leq \beta_i$. It follows that $\mathscr{V}(\boldsymbol{\gamma})$ is an admissible index-set.

Example 5.5. Of course $\{(\boldsymbol{\alpha}, i) \in {\mathbb{N}_0}^n \times \{1, \ldots, n\} \mid |\boldsymbol{\alpha}| > 1\}$ is an admissible index-set, the associate index-subgroup being the whole Nottingham group. In particular, using Remark 5.4, we find an embedding of the Nottingham group over R of rank r in the Nottingham group over R of rank n, whenever $r \leq n$

Example 5.6. Let $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_r$ be in ${\mathbb{N}_0}^n$. Then

$$\{(\boldsymbol{\beta}, i) \mid i \in \{1, \ldots, n\},\ \boldsymbol{\beta} \geq \boldsymbol{\alpha}_j \text{ for some } j \in \{1, \ldots, r\}\}$$

is an admissible index-set and the corresponding group is indeed $\mathcal{K}((\boldsymbol{t}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{t}^{\boldsymbol{\alpha}_r})) \cap \mathscr{G}\ell^1_n(R)$ where $\mathcal{K}((\boldsymbol{t}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{t}^{\boldsymbol{\alpha}_r}))$ is the subgroup associated to the ideal generated by $\boldsymbol{t}^{\boldsymbol{\alpha}_1}, \ldots, \boldsymbol{t}^{\boldsymbol{\alpha}_r}$ defined in Section 5.1.

Example 5.7. Let r be a positive integer less than n and let I be an admissible index-set in ${\mathbb{N}_0}^r \times \{1, \ldots, r\}$. Then $\bar{I}^n := \{((\boldsymbol{\alpha}, \alpha_{r+1}, \ldots, \alpha_n), i) \mid (\boldsymbol{\alpha}, i) \in I,\ \alpha_{r+1}, \ldots, \alpha_n \in \mathbb{N}_0\}$ is easily seen to be an admissible index-set.

Example 5.8. Let J be a non trivial subset of $\{1,\dots,n\}$ and fix a positive integer $s>1$. Consider the index-set

$$\mathscr{A}_s := \{(\boldsymbol{\alpha}, j) \in {\mathbb{N}_0}^n \times \{1,\dots,n\} \mid |\boldsymbol{\alpha}| \equiv_s 1\}$$

and let $(\boldsymbol{\alpha}_1, j_1)$ and $(\boldsymbol{\alpha}_2, j_2)$ be two pairs in it. Then for $i=1,2$ there exists a positive integer a_i such that $|\boldsymbol{\alpha}_i| = a_i s + 1$ and for every $h \in \mathbb{N}$

$$|h\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 - h\boldsymbol{\epsilon}_{i_1}| = h(|\boldsymbol{\alpha}|-1) + |\boldsymbol{\alpha}_2| = (ha_1 + a_2)s + 1$$

that is $(h\boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2 - h\boldsymbol{\epsilon}_{i_1}, i_2)$ is in the index-set which therefore is admissible.

Remark 5.7. So far we have not really used the hypothesis on the finite dimension of R over $\mathbb{F}_p$. Indeed, changing — very slightly — the definition of admissible index-set, we do not even need R to be an $\mathbb{F}_p$-algebra. According to this change it turns out that also pseudo-algebraic subgroups presented in Example 4.5 and Example 4.6 (to be more precise: their intersection with the Nottingham group) are index-subgroups. The next examples, instead, completely rely on R being an $\mathbb{F}_p$-algebra.

Example 5.9. For every $s \in \mathbb{N}$, define $\mathscr{C}_s$ to be the subset $\{(p^s\boldsymbol{\alpha}, i) \mid \boldsymbol{\alpha} \in {\mathbb{N}_0}^n,\ i \in \{1,\dots,n\}\}$ of ${\mathbb{N}_0}^n \times \{1,\dots,n\}$. Let $(p^s\boldsymbol{\alpha}, i)$ and $(p^s\boldsymbol{\beta}, j)$ be pairs in $\mathscr{C}_s$. Then, by Lemma B.4, any non-negative integer h such that $\binom{p^s\boldsymbol{\beta}}{h\boldsymbol{\epsilon}_i}$ is not equivalent to 0 modulo p is of the form $h = p^s k$. Thus $(kp^sp^s\boldsymbol{\alpha} + p^s\boldsymbol{\beta} - hp^s\boldsymbol{\epsilon}_i, j)$ is in $\mathscr{C}_s$. Note that when $s=1$, the resulting index-subgroup is the pseudo-algebraic subgroup associated to the trivial group (see Example 4.7).

Example 5.10. Let s be a fixed positive integer and consider the set Δ_s of n-tuples $\boldsymbol{\beta}$ in ${\mathbb{N}_0}^n$ such that $\mathbf{0} \le \boldsymbol{\beta} \le (p^s-1)\mathbf{1}$. It can be easily seen that, for every positive integer x such that $x \le |\Delta_s| = p^{sn}$, there exists a subset $X_x \subseteq \Delta_s$ of cardinality x such that any $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$ is in X_x whenever $\boldsymbol{\alpha} \le \boldsymbol{\beta}$ for some $\boldsymbol{\beta} \in X_x$. We define

$$\mathscr{C}_{s,X_x} := \{\big(p^{2s}\boldsymbol{\alpha} + p^s\boldsymbol{\beta}, i\big) \in {\mathbb{N}_0}^n \times \{1,\dots,n\} \mid i \in \{1,\dots,n\},\ \boldsymbol{\alpha},\boldsymbol{\beta} \in {\mathbb{N}_0}^n \text{ such that } \boldsymbol{\beta} \in X_x\}.$$

Let $\big(p^{2s}\boldsymbol{\alpha}_1 + p^s\boldsymbol{\beta}_1, i_1\big)$ and $\big(p^{2s}\boldsymbol{\alpha}_2 + p^s\boldsymbol{\beta}_2, i_2\big)$ be in $\mathscr{C}_{s,X_x}$. Let h be a non-negative integer such that $\binom{p^{2s}\boldsymbol{\alpha}_2 + p^s\boldsymbol{\beta}_2}{(h)\boldsymbol{\epsilon}_{i_1}}$ is not equivalent to 0 modulo p. Then, by Lemma B.4, we have that h is of the form $h = kp^{2s} + rp^s$ for some non-negative integers k and r such that $k\boldsymbol{\epsilon}_{i_1} \le \boldsymbol{\alpha}_2$ and $r\boldsymbol{\epsilon}_{i_1} \le \boldsymbol{\beta}_2$. Therefore

$$\begin{aligned}\boldsymbol{\gamma} = (kp^{2s} + rp^s)p^s\left(p^s\boldsymbol{\alpha}_1 + \boldsymbol{\beta}_1\right) + p^s\left(p^s\boldsymbol{\alpha}_2 + \boldsymbol{\beta}_2\right) - p^s(kp^s - r)\boldsymbol{\epsilon}_{i_1}\\ = p^{2s}\left((kp^s + r)(p^s\boldsymbol{\alpha}_1 + \boldsymbol{\beta}_1) + \boldsymbol{\alpha}_2 - k\boldsymbol{\epsilon}_{i_1}\right) + p^s\left(\boldsymbol{\beta}_2 - r\boldsymbol{\epsilon}_{i_1}\right)\end{aligned}$$

is such that $(\boldsymbol{\gamma}, i_2)$ is in $\mathscr{C}_{s,X_x}$, that is $\mathscr{C}_{s,X_x}$ is an admissible index-set. Note that $\mathscr{C}_{2s} = \mathscr{C}_{s,X_1}$.

5.2.1 Hausdorff spectrum of the Nottingham group

Here we generalize some arguments used in [3] to obtain some result about the Hausdorff spectrum of $\mathcal{G}\ell^1_n(R)$ with respect to the filtration $\{\mathcal{G}\ell^i_n(R) \mid i \in \mathbb{N}\}$.

Definition. For every $I \subseteq {\mathbb{N}_0}^n \times \{1,\dots,n\}$, we define the lower and upper density of I to be

$$\operatorname{ldense}(I) := \liminf_{j\in\mathbb{N}} \frac{|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j\}|}{n|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid 1 < |\boldsymbol{\alpha}| \le j\}|} \quad \text{and} \tag{5.4}$$

$$\operatorname{udense}(I) := \limsup_{j\in\mathbb{N}} \frac{|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j\}|}{n|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid 1 < |\boldsymbol{\alpha}| \le j\}|} \tag{5.5}$$

respectively. When they coincide, then we define the density of I to be $\operatorname{dense}(I) := \operatorname{ldense}(I) = \operatorname{udense}(I)$.

Remark 5.8. By Lemma B.1 and Lemma 1.2 the denominator in the definition of lower and upper density can be safely replaced by $\frac{nj^n}{(n!)} = \frac{j^n}{(n-1)!}$.

The interest in computing the density of an index-set is due to the following lemma.

Lemma 5.9. *Let I be an admissible index-set. Then the Hausdorff dimension of $\mathcal{J}(I)$ with respect to $\{\mathcal{Gl}^i_n(R) \mid i \in \mathbb{N}\}$ equals the lower density of I.*

Proof. By [4, Theorem 2.4], the Hausdorff dimension of $\mathcal{J}(I)$ equals

$$\liminf_{j\in\mathbb{N}} \frac{\log|\mathcal{J}(I)\mathcal{Gl}^j_n(R) : \mathcal{Gl}^j_n(R)|}{\log|\mathcal{Gl}^1_n(R) : \mathcal{Gl}^j_n(R)|} = \liminf_{j\in\mathbb{N}} \frac{\log|\mathcal{J}(I) : \mathcal{J}(I)\cap\mathcal{Gl}^j_n(R)|}{\log|\mathcal{Gl}^1_n(R) : \mathcal{Gl}^j_n(R)|}$$

where $\log_p|\mathcal{Gl}^1_n(R) : \mathcal{Gl}^j_n(R)| = n(\dim_{\mathbb{F}_p} R)|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid |\boldsymbol{\alpha}| \le j|$ by Corollary 1.20, while $\log_p|\mathcal{J}(I) : \mathcal{J}(I)\cap\mathcal{Gl}^j_n(R)| = (\dim_{\mathbb{F}_p} R)|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j\}|$, as, for every positive integer i, there exists a bijection between the quotient group of $\mathcal{J}(I)\cap\mathcal{Gl}^i_n(R)$ over $\mathcal{J}(I)\cap\mathcal{Gl}^{i+1}_n(R)$ and the free R-module generated by $\{\boldsymbol{t}^{\boldsymbol{\alpha}}\boldsymbol{E}_k \mid (\boldsymbol{\alpha}, k) \in I,\ |\boldsymbol{\alpha}| = i+1\}$ (see Corollary 1.20). □

Here we list some useful results about the density of index-sets.

Lemma 5.10. *Let I be a subset of ${\mathbb{N}_0}^n \times \{1, \ldots, n\}$. For every fixed integer d, we have*

$$\operatorname{ldense}(I) = \liminf_{j\ge|d|} \frac{|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j+d\}|}{n|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid |\boldsymbol{\alpha}| \le j\}|}$$
$$\operatorname{udense}(I) = \limsup_{j\ge|d|} \frac{|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j+d\}|}{n|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid |\boldsymbol{\alpha}| \le j\}|}$$

Proof. Assume d is positive. Then $|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j+d\}|$ is clearly less than

$$|\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j\}| + n\sum_{l=j+1}^{d}\binom{l+n-1}{n-1}$$

where — by Lemma B.1 — the term $n\sum_{l=j+1}^{j+d}\binom{j+n-1}{n-1}$ is at most $((j+d+n)^n - (d+n)^n)/n!$, that is a polynomial of degree $n-1$ with respect to j, whereas $|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid |\boldsymbol{\alpha}| \le j\}|$ is asymptotic to a polynomial of degree n. Thus $n\sum_{l=j+1}^{j+d}\binom{j+n-1}{n-1}$ is irrelevant in the computation of the limits. Similarly we find a lower bound and the same can be done for a negative d. □

Lemma 5.11. *Let I be a subset of ${\mathbb{N}_0}^n \times \{1, \ldots, n\}$ and fix $\boldsymbol{\delta} \in {\mathbb{N}_0}^n$. Then the lower (resp. upper) density of I coincides with the lower (resp. upper) density of $J := \{(\boldsymbol{\alpha}+\boldsymbol{\delta}, i) \mid (\boldsymbol{\alpha}, i) \in I\}$.*

Proof. This follows from the previous lemma and from the formula

$$|\{(\boldsymbol{\alpha}, i) \in J \mid |\boldsymbol{\alpha}| \le j\}| = |\{(\boldsymbol{\alpha}+\boldsymbol{\delta}, i) \mid (\boldsymbol{\alpha}, i) \in I,\ |\boldsymbol{\alpha}| + |\boldsymbol{\delta}| \le j\}| = |\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \le j - |\boldsymbol{\delta}|\}|$$

that holds for every positive integer $j > |\boldsymbol{\delta}|$. □

Lemma 5.12. *Let I be a subset of ${\mathbb{N}_0}^n \times \{1, \ldots, n\}$. For every positive integer s, we have*

$$\operatorname{ldense}(I) = \liminf_{j\in\mathbb{N}} \frac{|\{(p^s\boldsymbol{\alpha}+\boldsymbol{\beta}, i) \in I \mid p^s|\boldsymbol{\alpha}| \le j \text{ and } \mathbf{0} \le \boldsymbol{\beta} \le (p^s-1)\mathbf{1}\}|}{n|\{p^s\boldsymbol{\alpha}+\boldsymbol{\beta} \in {\mathbb{N}_0}^n \mid p^s|\boldsymbol{\alpha}| \le j \text{ and } \mathbf{0} \le \boldsymbol{\beta} \le (p^s-1)\mathbf{1}\}|}$$
$$\operatorname{udense}(I) = \limsup_{j\in\mathbb{N}} \frac{|\{(p^s\boldsymbol{\alpha}+\boldsymbol{\beta}, i) \in I \mid p^s|\boldsymbol{\alpha}| \le j \text{ and } \mathbf{0} \le \boldsymbol{\beta} \le (p^s-1)\mathbf{1}\}|}{n|\{p^s\boldsymbol{\alpha}+\boldsymbol{\beta} \in {\mathbb{N}_0}^n \mid p^s|\boldsymbol{\alpha}| \le j \text{ and } \mathbf{0} \le \boldsymbol{\beta} \le (p^s-1)\mathbf{1}\}|}$$

Proof. This also follows from Lemma 5.10, as

$$\begin{aligned}\{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \leq j - np^s\} &\subseteq \\ &\subseteq \{(p^s\boldsymbol{\alpha} + \boldsymbol{\beta}, i) \in I \mid p^s|\boldsymbol{\alpha}| \leq j \text{ and } \mathbf{0} \leq \boldsymbol{\beta} \leq (p^s - 1)\mathbf{1}\} \subseteq \\ &\subseteq \{(\boldsymbol{\alpha}, i) \in I \mid |\boldsymbol{\alpha}| \leq j + np^s\}\end{aligned}$$

for every $j \geq np^s$ and the same holds substituting ${\mathbb{N}_0}^n \times \{1, \ldots, n\}$ to I. □

Now we are able to compute some Hausdorff dimensions of the index-subgroups presented in the examples. Index-sets in Example 5.4 and 5.6 have density 1, by Lemma 5.11.

In Example 5.5, we showed there exists an index-subgroup of $\mathcal{Gl}^1_n(R)$ isomorphic to the generalized Nottingham group of rank m, for every $m \leq n$. The (lower) density of the associated index-set I_m is

$$\operatorname{ldense}(I_m) = \liminf_{j \in \mathbb{N}} \frac{m|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^m \mid |\boldsymbol{\alpha} \leq j\}|}{n|\{\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \mid |\boldsymbol{\alpha}| \leq j} = \liminf_{j \in \mathbb{N}} \frac{(n-1)! j^m}{(m-1)! j^n}$$

that is zero whenever $m < n$.

Let s be a positive integer. For every $\boldsymbol{\gamma} \in {\mathbb{N}_0}^n$, consider the set $C_{\boldsymbol{\gamma}} := \{p^{2s}\boldsymbol{\gamma} + \boldsymbol{\beta} \in {\mathbb{N}_0}^n \mid \mathbf{0} \leq \boldsymbol{\beta} \leq (p^s - 1)\mathbf{1}\}$, that is the p^s-cell of vertex $p^s\boldsymbol{\gamma}$, as defined in Chapter 6, Section 6.1. Fix $1 \leq x \leq p^{sn}$ and let X_x be a set as described in Example 5.10. The pairs $(\boldsymbol{\alpha}, i) \in \mathscr{C}_{s,X_x}$ such that $\boldsymbol{\alpha}$ is in $C_{\boldsymbol{\gamma}}$ are exactly $n|X_x| = nx$. Thus, using Lemma 5.12, the density of $\mathscr{C}_{s,x}$ is x/p^{2sn}. Note that x/p^{2sn} is always less than $1/np$. Similarly the density of $\mathscr{C}_s$ is $1/p^{sn}$.

It remains to study Example 5.8 and Example 5.7. So let s be again a fixed positive integer. Then, by Lemma B.1,

$$|\{(\boldsymbol{\alpha}, i) \in \mathscr{A}_s \mid |\boldsymbol{\alpha}| \leq j\}| = n \sum_{k=1}^{\lfloor (j-1)/s \rfloor} \binom{ks + n}{n - 1}$$

is asymptotic to $nj^n/(n!s)$ and therefore the density of $\mathscr{A}_s$ is

$$\lim_{j \in \mathbb{N}} \frac{nj^n/(n!s)}{nj^n/n!} = \frac{1}{s}$$

Finally, for index-sets of Example 5.7 we have the most interesting result of this section:

Proposition 5.13. *Let I be an admissible index-set in ${\mathbb{N}_0}^n$ of density d. Then the set $\bar{I}^{n+1}$ — where $\bar{I}^{n+1}$ is the index-set defined in Example 5.7 — has density equal to $dn/(n+1)$.*

Proof. Let us introduce the following notation: for every positive integer j, by I_j (and $\bar{I}^{n+1}_j$) we mean the set of pairs $(\boldsymbol{\alpha}, i)$ in I (resp. $\bar{I}^{n+1}_j$) such that $\boldsymbol{\alpha}$ has weight less than $j + 1$. By hypothesis, the limit for j that tends to infinity of $((n-1)!|I_j|)/j^n$ exists and it is equal to d. It follows that there exist polynomials $f(x), g(x) \in \mathbb{R}[x]$ of degree n and leading coefficient $d/(n-1)!$ such that $f(j) \leq |I_j| \leq g(j)$ for every $j \in \mathbb{N}$. We want to prove that the limit of $\left(n!|\bar{I}^{n+1}_J|\right)/j^{n+1}$ also exists and it is equal to $dn/(n+1)$.

For every $j \in \mathbb{N}$, the set $\bar{I}^{n+1}_j$ can be trivially decomposed as disjoint union — as k ranges over $2, \ldots, j$ — of subsets $\bar{I}^{n+1}_k \setminus \bar{I}^{n+1}_{k-1}$, each of which equals

$$\begin{aligned}\left\{((\boldsymbol{\alpha}, \alpha_{n+1}), i) \in {\mathbb{N}_0}^{n+1} \times \{1, \ldots, n+1\} \mid (\boldsymbol{\alpha}, i) \in I,\ \alpha_{n+1} \in \mathbb{N}_0 \text{ and } |\boldsymbol{\alpha}| + \alpha_{n+1} = k\right\} &= \\ = \left\{((\boldsymbol{\alpha}, k - |\boldsymbol{\alpha}|), i) \in {\mathbb{N}_0}^{n+1} \times \{1, \ldots, n+1\} \mid (\boldsymbol{\alpha}, i) \in I_k\right\}&\end{aligned}$$

and in particular has the same cardinality of $|I_k|$. Thus we have $|\bar{I}_j^{n+1}| = \sum_{k=2}^{j} |I_k|$. Let $\bar{k}$ be a positive integer such that $g(x)$ is non-decreasing in $[\bar{k}, \infty)$ and let c denote $\sum_{k=2}^{\bar{k}-1} g(k)$. Using standard integral arguments, we obtain, for every $j \geq \bar{k}$,

$$|\bar{I}_j^{n+1}| \leq c + \sum_{k=\bar{k}}^{j} g(k) \leq c + \int_{\bar{k}}^{j+1} g(x)\mathrm{d}x = c + \int_{\bar{k}}^{j+1} \left(\frac{dj^n}{(n-1)!} + [\ldots] \right) \mathrm{d}x =$$

$$= \frac{dj^{n+1}}{(n+1)(n-1)!} + [\ldots]$$

where we omitted lower degree terms. Similarly, we may prove that there exists a polynomial lower-bound $\frac{dj^{n+1}}{(n+1)(n-1)!} + [\ldots]$ for $|\bar{I}_j^{n+1}|$, that therefore is actually asymptotic to $\frac{dj^{n+1}}{(n+1)(n-1)!}$ as j tends to infinity. It follows that

$$\lim_{j \in \mathbb{N}} \frac{n! |\bar{I}_j^{n+1}|}{j^{n+1}} = \lim_{j \in \mathbb{N}} \frac{n!\ d}{(n+1)(n-1)!} = d \frac{n}{n+1},$$

whence the claim follows. □

Corollary 5.14. *Let m be a positive integer greater than n, and let I be an index-set in ${\mathbb{N}_0}^n \times \{1, \ldots, n\}$ of density d. Then there exists an index-set in ${\mathbb{N}_0}^m \times \{1, \ldots, m\}$ of density dn/m.*

This corollary is a strong tool to compute pieces of the Hausdorff spectrum of the generalized Nottingham group. Indeed, perhaps one of the main results in the paper [3] is the following theorem.

Theorem 5.15 (Theorem 1.8, [3]). *If $p > 2$, the set of Hausdorff dimensions of index-subgroups of the (classic) Nottingham group over a p-characteristic finite field $\mathbb{F}_q$ with respect to $\{\mathcal{G}\ell_1^i(\mathbb{F}_q) \mid i \in \mathbb{N}\}$ is*

$$\text{inspec}(\mathcal{G}\ell_1^1(\mathbb{F}_q)) := \left[0, \frac{1}{p}\right] \cup \left\{ \frac{1}{p} + \frac{1}{p^r} \mid r \in \mathbb{N} \right\} \cup \left\{ \frac{1}{s} \mid s \in \mathbb{N} \right\}$$

To prove it, Barnea and Klopsch exhibit explicit index-sets whose density is ζ for each $\zeta \in$ inspec. Thus we immediately obtain the following

Theorem 5.16. *The Hausdorff spectrum of the generalized Nottingham group of rank n over a finite field of odd characteristic contains*

$$\left[0, \frac{1}{np}\right] \cup \left\{ \frac{1}{np} + \frac{1}{np^r} \mid r \in \mathbb{N} \right\} \cup \left\{ \frac{j}{ns} \mid j \in \{1, \ldots, n\},\ s \in \mathbb{N} \right\}$$

Proof. This theorem is an immediate consequence of Theorem 5.15 and Proposition 5.13. We just remark that to obtain an admissible index-set of density $j/(ns)$, we take $\mathscr{A}_s$ in ${\mathbb{N}_0}^j \times \{1, \ldots, j\}$ and then we extend it to ${\mathbb{N}_0}^n \times \{1, \ldots, n\}$. □

Part III

The generalized Nottingham group over a finite field

Chapter 6

Just infiniteness of the Nottingham group

In this chapter we are going to prove our main result, namely that the generalized Nottingham group is hereditarily just infinite. As already said, the motivating reason to introduce the generalized Nottingham group was finding new just infinite groups. The original definition [34] was given for the Nottingham group over a finite field of prime order, whereas in Chapter 1 we gave a more general definition. However for this particular purpose it makes sense to restrict to finite fields only, as the next results show.

Proposition 6.1. *The generalized Nottingham group over R is profinite if and only if R is profinite.*

Proof. If R is profinite, then it is compact and has a base for the neighbourhoods of 0 given by open and closed ideals [33, Proposition 5.1.2.(d)]. It follows that $\mathcal{G}\ell^1_n(R)$ is compact and Hausdorff, topologically being a countable Cartesian product of R with itself. Moreover, every open neighbourhood of the identity has to contain a subset of the form

$$\{(t_i + \sum_{\boldsymbol{\alpha} \in \mathbb{N}_0{}^n} f_{i,\boldsymbol{\alpha}} \boldsymbol{t}^{\boldsymbol{\alpha}})_{i=1}^n \in \mathcal{G}\ell^1_n(R) \mid f_{i,\boldsymbol{\alpha}} \in I \text{ for every } |\boldsymbol{\alpha}| < j\}$$

for some $j \in \mathbb{N}$ and open ideal I. But such a subset coincides with the normal closed subgroup defined in Lemma 4.8, that is $\mathcal{G}\ell^1_n(R)$ has a base for the open neighbourhoods of the identity given by normal subgroups.

Conversely, if R is not profinite, then $\mathcal{G}\ell^1_n(R)$ it is not compact because R itself is not compact [33, Proposition 5.1.2.(b)]. □

Proposition 6.2. *If $\mathcal{G}\ell^1_n(R)$ is a just infinite profinite group, then R is a finite field.*

Proof. Because of the previous proposition, the ring R is profinite. If it had a proper non-trivial ideal, then the associated closed normal subgroup defined in Lemma 4.8 would have infinite index. Thus R is a field, but a topological field is compact if and only it is finite (this may be considered a consequence of [33, Proposition 5.1.2] as well). □

Our proof of just infiniteness for the generalized Nottingham group holds only for odd characteristic field. The statement is probably true for even characteristic fields too; however, as for the classical Nottingham group, the proofs should rely on different ideas. In particular, one should find a suitable replacement for Lemma 6.7.

Thus we fix an odd prime p, a p-power q and the field $\mathbb{F}_q$ of order q. Since the "classic" Nottingham group it is well known to be hereditarily just infinite, we also assume $n > 1$.

We proceed through four stages, whose results may appear quite technical, but that indeed have a nice visual interpretation. So, to better clarify the underlying ideas, we will alternate actual proofs to examples in the particular case when $n = 2$ and $p = q = 3$.

Notation 19. Since R and n are fixed, instead of $\mathcal{M}_n(\mathbb{F}_q)$, $\mathcal{M}_n^i(\mathbb{F}_q)$, $\mathcal{G}\ell_n^1(\mathbb{F}_q, n)$ and $\mathcal{G}\ell_n^i$ we will just write $\mathcal{M}$, $\mathcal{M}^i$, $\mathcal{G}\ell_n^1$ and $\mathcal{G}\ell_n^i$ respectively.

6.1 Technical notation and visual representation

We already defined the support of a formal power series in Chapter 1 (Subsection 1.1.1), of an element of the generalized Nottingham group (equation 5.1) and its restricted version (equation 5.2). The reader is invited to look back at them as they are going to be a fundamental tool.

For every $l \in \mathbb{N}_0$, we introduce a function $\Psi_l : {\mathbb{N}_0}^n \to {\mathbb{N}_0}^n$ such that, for every $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$,

$$\Psi_l(\boldsymbol{\alpha}) := \max\{\boldsymbol{\beta} \in {\mathbb{N}_0}^n \mid p^l \boldsymbol{\beta} \leq \boldsymbol{\alpha}\} \tag{6.1}$$

while for every $s, l, d \in \mathbb{N}_0$ and for every $\boldsymbol{\chi} \in {\mathbb{N}_0}^n$, we define the sets

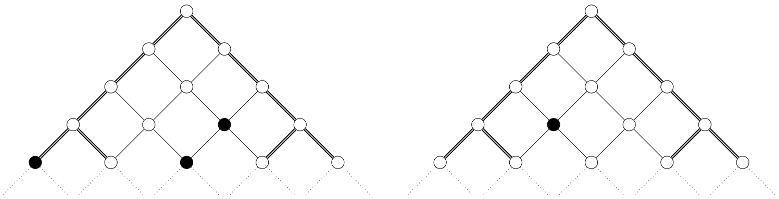
$$\begin{aligned}\mathsf{S}(l,\ d) &:= \{\boldsymbol{f} \in \mathcal{G}\ell_n^1 \mid p^l \Psi_l(\boldsymbol{\alpha}) = \boldsymbol{\alpha} \quad \text{for all } (\boldsymbol{\alpha}, i) \in \operatorname{Supp}_d(\boldsymbol{f})\}\\ \mathsf{D}(s,\ \boldsymbol{\chi}) &:= \{\boldsymbol{f} \in \mathcal{G}\ell_n^1 \mid \Psi_s(\boldsymbol{\alpha}) = \boldsymbol{\chi} \quad \text{for all } (\boldsymbol{\alpha}, i) \in \operatorname{Supp}_1(\boldsymbol{f})\}\end{aligned}$$

that will be later useful. Note that $\boldsymbol{f} \in \mathcal{G}\ell_n^1$ is in $\mathsf{S}(l,\ d)$ if and only if there exists $\boldsymbol{g} \in \mathcal{M}^1$ such that $\boldsymbol{f} \equiv \boldsymbol{t} + \boldsymbol{g}^{p^l}$ modulo $\mathcal{M}^{\omega(\boldsymbol{f})+d+1}$, in other words, if and only if $\boldsymbol{f} \in \mathcal{I}(\mathscr{C}_l)\mathcal{G}\ell_n^{\omega(\boldsymbol{f})+d}$, where $\mathcal{I}(\mathscr{C}_l)$ is the index-subgroup related to Example 5.9.

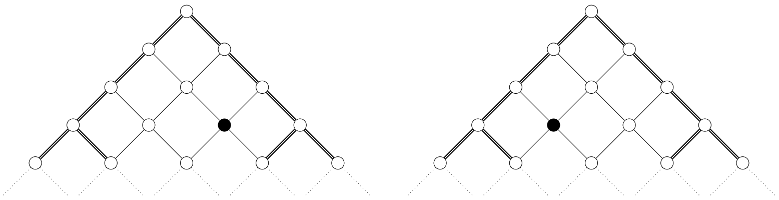
Example 6.1. The support of an element can be seen as a vertices subset of the graph given by n copies of the Cayley graph of ${\mathbb{N}_0}^n$, a picture of which has been given in Example 1.1. So, for $n = 2$, the element $\boldsymbol{f} = (t_i + f_i) \in \mathcal{G}\ell_n^1$ defined by

$$\boldsymbol{f} = \begin{pmatrix} t_1 + t_1 t_2^2 + t_1^2 t_2^2 + t_1^4 \\ t_2 + t_1^2 t_2 \end{pmatrix}$$

has support represented by



The restricted 1-support is $\{((0,3),1), ((2,1),2)\}$ and corresponds to the first line with at least one black dot, i. e.



Moreover $\boldsymbol{f}$ is in $\mathsf{D}\,(1,\ \mathbf{0})$.

In the graphs in the example, we doubled lines corresponding to the sublattice $p\mathbb{N}_0{}^n = \{p\boldsymbol{\alpha} \mid \boldsymbol{\alpha} \in \mathbb{N}_0{}^n\}$ of $\mathbb{N}_0{}^n$, that will turn out to have an important role in our proof, as well as all sublattices of the form $p^l\mathbb{N}_0{}^n$ for $l \in \mathbb{N}$. Call p^l-cell with vertex $p^l\boldsymbol{\chi}$ the subset $\{\boldsymbol{\alpha} \in \mathbb{N}_0{}^n \mid p^l\boldsymbol{\chi} \le \boldsymbol{\alpha} \le p^l\boldsymbol{\chi} + p^{l-1}(p-1)\mathbf{1}\}$. Then doubled line in previous graphs determine the boundary of p-cells (more precisely, each double line belongs to the p-cell below). In this language $\boldsymbol{f} \in \mathcal{G}\ell_n^1$ is in $\mathsf{D}\,(s,\ \boldsymbol{\chi})$ if and only if its restricted 1-support is contained in the union of the n p^s-cells — one for each copy of the Cayley graph — with vertex $p^s\boldsymbol{\chi}$ and it is in $\mathsf{S}\,(l,\ d)$ if and only if its restricted d-support lies on $p^l\mathbb{N}_0{}^n$.

Lemma 6.3. *Let l and s be non-negative integers such that $l \le s$. Then*

(i) $\Psi_s\,(\boldsymbol{\alpha} + p^s\boldsymbol{\beta}) = \Psi_s\,(\boldsymbol{\alpha}) + \boldsymbol{\beta}$ *for every* $\boldsymbol{\alpha}\ \boldsymbol{\beta} \in \mathbb{N}_0{}^n$*;*

(ii) $\Psi_s\,(p^l\boldsymbol{\alpha}) = \Psi_{s-l}\,(\boldsymbol{\alpha})$ *for every* $\boldsymbol{\alpha} \in \mathbb{N}_0{}^n$*;*

(iii) $\Psi_s\,(p\boldsymbol{\alpha} + \boldsymbol{\beta}) = \Psi_s\,(p\boldsymbol{\alpha})$ *for every* $\boldsymbol{\alpha} \in \mathbb{N}_0{}^n$ *and every* $\boldsymbol{\beta} \in \mathbb{N}_0{}^n$ *such that* $\boldsymbol{\beta} \le (p-1)\mathbf{1}$*;*

(iv) $\Psi_s\,(p^l\boldsymbol{\alpha} + \boldsymbol{\beta}) = \Psi_s\,(p^l\boldsymbol{\alpha})$ *for every* $\boldsymbol{\alpha} \in \mathbb{N}_0{}^n$ *and every* $\boldsymbol{\beta} \in \mathbb{N}_0{}^n$ *such that* $\boldsymbol{\beta} \le (p^l-1)\mathbf{1}$*;*

(v) if $\boldsymbol{\alpha}$ *and* $\boldsymbol{\beta}$ *in* $\mathbb{N}_0{}^n$ *are such that* $\Psi_s\,(p^s\boldsymbol{\alpha} + \boldsymbol{\beta}) = \boldsymbol{\alpha}$*, then* $\boldsymbol{\beta} \le (p^s-1)\mathbf{1}$*.*

Proof. Let $\boldsymbol{\gamma}$ be in $\mathbb{N}_0{}^n$. Then $p^s\boldsymbol{\gamma} \le \boldsymbol{\alpha}$ if and only if $p^s\boldsymbol{\gamma} + p^s\boldsymbol{\beta} \le \boldsymbol{\alpha} + p^s\boldsymbol{\beta}$, whence the first part of the statement follows.

For the second part, note that $p^s\boldsymbol{\gamma} \le p^l\boldsymbol{\alpha}$ if and only if $p^l(\boldsymbol{\alpha} - p^{s-l}\boldsymbol{\gamma}) \ge 0$, i. e. if and only if $\boldsymbol{\alpha} \ge p^{s-l}\boldsymbol{\gamma}$.

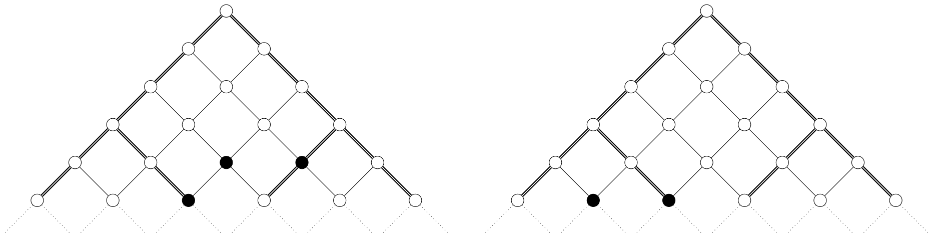
The fourth statement can be proved by induction using (iii) and (ii), while we prove (iii) by showing that $\Psi_s\,(p\boldsymbol{\alpha} + \boldsymbol{\beta}) \le \Psi_s\,(p\boldsymbol{\alpha})$, the converse being trivial. So, let $\boldsymbol{\gamma} \in \mathbb{N}_0{}^n$ be such that $p^s\boldsymbol{\gamma} \le p\boldsymbol{\alpha} + \boldsymbol{\beta}$. Then $p(p^{s-1}\boldsymbol{\gamma} - \boldsymbol{\alpha}) \le \boldsymbol{\beta} \le (p-1)\mathbf{1}$ that might hold only if $p^s\boldsymbol{\gamma} \le p\boldsymbol{\alpha}$, whence $\Psi_s\,(p\boldsymbol{\alpha} + \boldsymbol{\beta}) \le \Psi_s\,(p\boldsymbol{\alpha})$.

Finally, assume $\boldsymbol{\beta} \not\le (p^s-1)\mathbf{1}$ then there exists $j \in \{1, \dots, n\}$ such that $\boldsymbol{\beta} \ge p^s\boldsymbol{\epsilon}_j$ and therefore $\Psi_s\,(p^s\boldsymbol{\alpha} + \boldsymbol{\beta}) \ge \Psi_s\,(p^s\boldsymbol{\alpha} + p^s\boldsymbol{\epsilon}_j)$ that equals $\boldsymbol{\alpha} + \boldsymbol{\epsilon}_j$ by (i) and (ii). □

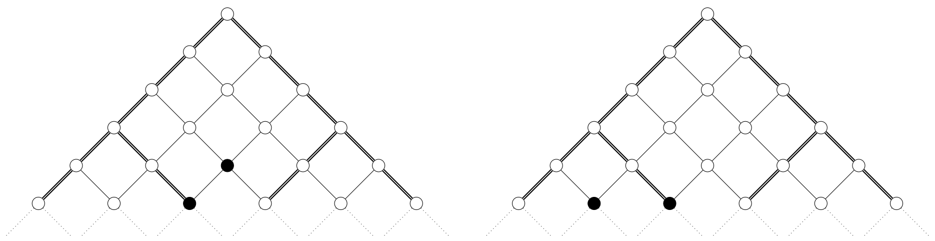
The very last technical tool we need is the following. Fix a non-negative integer l and a positive integer d_0. Let $\boldsymbol{\omega}$ be in $\mathbb{N}_0{}^n$. Then for every $f \in \mathbb{F}_q[\![\boldsymbol{t}]\!]$ we define

$$\mathsf{A}\,(l,\ \boldsymbol{\omega},\ \boldsymbol{f},\ d_0) := \{(\boldsymbol{\alpha}, i) \in \operatorname{Supp}_{d_0}\boldsymbol{f} \mid \boldsymbol{\alpha} \ge p^l\boldsymbol{\omega} \text{ and } \Psi_{l+1}\,(\boldsymbol{\alpha}) = \Psi_{l+1}\,(\boldsymbol{\alpha} - p^l\boldsymbol{\omega})\}$$

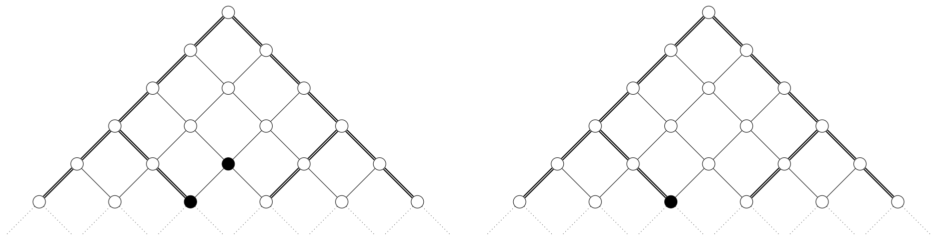
Example 6.2. Again, the meaning of this last definition will be better explained by an illustration. Assume $\boldsymbol{f}$ is an element in $\mathcal{G}\ell_n^1$ whose support is represented by



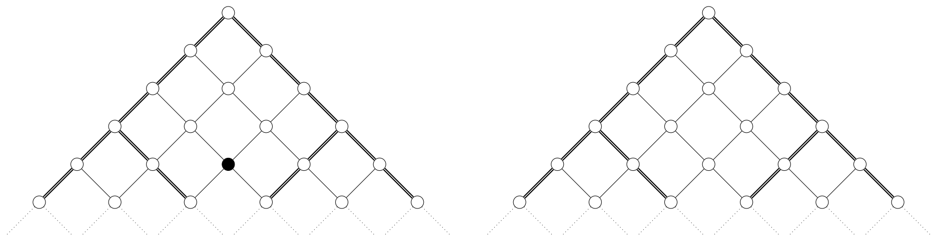
where single lines denote the lattice $p^l\mathbb{N}$ whereas double lines denote the lattice $p^{l+1}\mathbb{N}$. Then $\mathsf{A}\,(l,\ \boldsymbol{\epsilon}_2,\ \boldsymbol{f},\ 2)$ is represented by



while $\mathsf{A}\left(l,\ 2\boldsymbol{\epsilon}_2,\ \boldsymbol{f},\ 2\right)$ is represented by



and $\mathsf{A}\left(l,\ 2\boldsymbol{\epsilon}_1,\ \boldsymbol{f},\ 2\right)$



From these examples it might be clear what is the general rule: the only surviving dots are those that do not cross double lines when moving backward along with $\boldsymbol{\omega}$. In particular, when $\boldsymbol{f}$ is in $\mathsf{S}\left(l,\ d_0\right)$, the set $\mathsf{A}\left(l,\ \boldsymbol{\omega},\ \boldsymbol{f},\ d_0\right)$ is empty whenever $\boldsymbol{\omega} \not\leq (p-1)\mathbf{1}$ and $\mathsf{A}\left(l,\ (p-1)\mathbf{1},\ \boldsymbol{f},\ d_0\right)$ only contains dots that are in the deepest corner of their p^l-cell. The next lemma formalizes these intuitions.

Lemma 6.4. *Let $\boldsymbol{\alpha} \geq \boldsymbol{\omega}$ be in ${\mathbb{N}_0}^n$, and let s be a non-negative integer. Then $\Psi_s\left(\boldsymbol{\alpha}\right) = \Psi_s\left(\boldsymbol{\alpha} - p^s\boldsymbol{\omega}\right)$ if and only if there exists $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$ such that $p^s\boldsymbol{\omega} \leq \boldsymbol{\beta} \leq (p^s-1)\mathbf{1}$ and $\boldsymbol{\alpha} = p^s\Psi_s\left(\boldsymbol{\alpha}\right) + \boldsymbol{\beta}$.*

Proof. Let $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$ be $\boldsymbol{\alpha} - p^s\Psi_s\left(\boldsymbol{\alpha}\right)$. It is well defined since $\boldsymbol{\alpha} \geq p^s\Psi_s\left(\boldsymbol{\alpha}\right)$ by definition and it is less than or equal to $(p^s-1)\mathbf{1}$ by Lemma 6.3, statement (v). Then $\Psi_s\left(\boldsymbol{\alpha} - p^s\boldsymbol{\omega}\right)$ is equal to $\Psi_s\left(p^s\Psi_s\left(\boldsymbol{\alpha}\right) + \boldsymbol{\beta} - p^s\boldsymbol{\omega}\right)$ that equals $\Psi_s\left(\boldsymbol{\alpha}\right)$ if and only if $\mathbf{0} \leq \boldsymbol{\beta} - p^s\boldsymbol{\omega} \leq (p^s-1)\mathbf{1}$, whence the claim follows. □

Note that if we know that $\boldsymbol{\alpha} = p^l\boldsymbol{\alpha}'$ for some $l \leq s$ and some $\boldsymbol{\alpha}' \in {\mathbb{N}_0}^n$, then $\boldsymbol{\beta} = p^l\boldsymbol{\beta}'$ for some $\boldsymbol{\beta}' \in {\mathbb{N}_0}^n$ and we can sharpen the upper bound to $p^l(p^{s-l}-1)\mathbf{1}$. In particular, when $s = l+1$, we have $\Psi_{l+1}\left(\boldsymbol{\alpha}\right) = \Psi_{l+1}\left(\boldsymbol{\alpha} - p^l(p-1)\mathbf{1}\right)$ if and only if $\boldsymbol{\alpha} = p^s\Psi_s\left(\boldsymbol{\alpha}\right) + p^l(p-1)\mathbf{1}$. So, we have obtained

Corollary 6.5. *Let d_0 and l be non-negative integers and let $\boldsymbol{f} \in \mathcal{G}l_n^1$ be in $\mathsf{S}\left(l,\ d_0\right)$. Then a pair $(\boldsymbol{\alpha}, i)$ in the restricted d_0-support of $\boldsymbol{f}$ is in $\mathsf{A}\left(l,\ (p-1)\mathbf{1},\ \boldsymbol{f},\ d_0\right)$ if and only if $\boldsymbol{\alpha}$ equals $p^{l+1}\Psi_{l+1}\left(p^l\boldsymbol{\alpha}\right) + p^l(p-1)\mathbf{1}$.*

Remark 6.6. Let $(c_i)_{i=1}^{|\boldsymbol{\omega}|} \in \{1, \ldots, n\}^{|\boldsymbol{\omega}|}$ be such that $\boldsymbol{\omega} = \sum_{i=1}^{|\boldsymbol{\omega}|} \boldsymbol{\epsilon}_{c_i}$. Then, by Lemma B.4, we have that for every $\boldsymbol{\alpha} = (\alpha_i)_{i=1}^n \in {\mathbb{N}_0}^n$ such that $\boldsymbol{\alpha} \geq p^l \boldsymbol{\omega}$

$$\partial_{p^l \boldsymbol{\epsilon}_{c_1}} \partial_{p^l \boldsymbol{\epsilon}_{c_2}} \ldots \partial_{p^l \boldsymbol{\epsilon}_{|\boldsymbol{\omega}|}} \boldsymbol{t}^{\boldsymbol{\alpha}} = \frac{\boldsymbol{\alpha}'!}{(\boldsymbol{\alpha}' - \boldsymbol{\omega})!} \boldsymbol{t}^{\boldsymbol{\alpha} - p^l \boldsymbol{\omega}}$$

where $\boldsymbol{\alpha}' = (\lfloor \alpha_i / p^l \rfloor)_{i=1}^n \in {\mathbb{N}_0}^n$. Thus $\partial_{p^l \boldsymbol{\epsilon}_{c_1}} \partial_{p^l \boldsymbol{\epsilon}_{c_2}} \ldots \partial_{p^l \boldsymbol{\epsilon}_{|\boldsymbol{\omega}|}} \boldsymbol{t}^{\boldsymbol{\alpha}}$ is not zero if and only if p does not divide $\boldsymbol{\alpha}'!/(\boldsymbol{\alpha}' - \boldsymbol{\omega})! \in \mathbb{Z}$, i. e. if and only if $\varPsi_1(\boldsymbol{\alpha}' - \boldsymbol{\omega}) = \varPsi_1(\boldsymbol{\alpha}')$ (from a graphical point of view this means $\boldsymbol{\alpha} - p^l \boldsymbol{\omega}$ and $\boldsymbol{\alpha}$ lay in the same p^{l+1}-cell). It follows that $(\boldsymbol{\alpha}, i) \in \mathrm{Supp}_{d_0} \boldsymbol{f}$ is in $\mathsf{A}(l, \boldsymbol{\omega}, \boldsymbol{f}, d_0)$ if and only if $\partial_{p^l \boldsymbol{\epsilon}_{c_1}} \partial_{p^l \boldsymbol{\epsilon}_{c_2}} \ldots \partial_{p^l \boldsymbol{\epsilon}_{|\boldsymbol{\omega}|}} \boldsymbol{t}^{\boldsymbol{\alpha}}$ is not 0.

6.2 Basic stages of the proof

As already mentioned, the proof is based on four stages that allow to play with the restricted support of elements. That is to say, given a non-trivial element in a normal subgroup of an open subgroup of $\mathcal{G}\ell_n^1$, we prescribe some modification that can be achieved in the restricted support, by taking other elements in the same normal subgroup.

Each stage here gives a particular rule and it is independent from the others.

Notation 20. From now on we fix an open subgroup O containing $\mathcal{G}\ell_n^m$, where m is some positive integer, a closed normal subgroup N of O and a non-trivial element $\boldsymbol{f} \in N$.

First stage

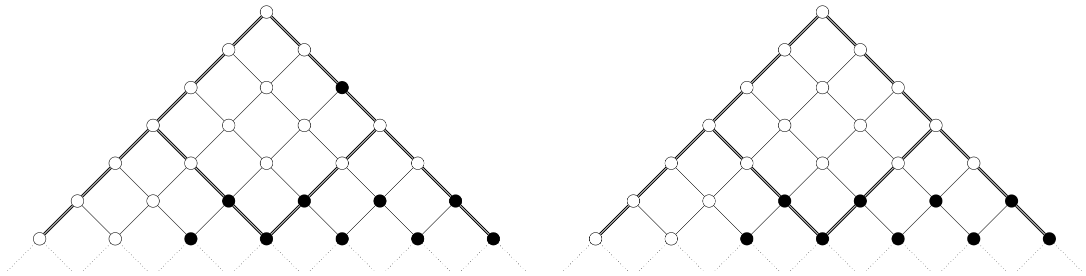
Lemma 6.7. *Fix $i \in \{1, \ldots, n\}$ and $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$. Then, for every $j \in \{1, \ldots, n\}$ and every $\boldsymbol{\delta} \in {\mathbb{N}_0}^n$ such that $|\boldsymbol{\delta}| \geq 2m + 2$, there exist $D_1, D_2, D_3, D_4 \in \mathrm{Der}_m(\mathbb{F}_q[\![\boldsymbol{t}]\!])$ such that $\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}} \partial_j = [[\boldsymbol{t}^{\boldsymbol{\alpha}} \partial_i, D_1], D_2] + [[\boldsymbol{t}^{\boldsymbol{\alpha}} \partial_i, D_3], D_4]$.*

Before approaching its proof, let us see what is the meaning of this lemma. Note that by linearity of Lie brackets, such a result implies that any element of the form $r\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}} \partial_j$ — where $r \in \mathbb{F}_q$, $i \in \{1, \ldots, n\}$, $|\boldsymbol{\delta}| \geq 2m + 2$ — is in the ideal generated by $\boldsymbol{t}^{\boldsymbol{\alpha}} \partial_i$ in any subalgebra of $L(\mathcal{G}\ell_n^1)$ containing $L_{\mathcal{G}\ell_n^1}(\mathcal{G}\ell_n^m) \cong \mathrm{Der}_R^m(R[\![\boldsymbol{t}]\!])$. In particular such an ideal contains the Lie subalgebra

$$\left\{ \sum_{i=1}^n f_i \partial_i \mid f_i \in (\boldsymbol{t}^{\boldsymbol{\alpha}}) \trianglelefteq \mathbb{F}_q[\![\boldsymbol{t}]\!] \right\} \cap \mathrm{Der}_{|\boldsymbol{\alpha}|+2m+1}(\mathbb{F}_q[\![\boldsymbol{t}]\!]).$$

In terms of groups: if $\boldsymbol{f} \in N$ is such that $\iota_{\mathcal{G}\ell_n^1}(\boldsymbol{f}) = \boldsymbol{t}^{\boldsymbol{\alpha}} \partial_i$ (recall that $\iota_{\mathcal{G}\ell_n^1}$ is the map from $\mathcal{G}\ell_n^1$ to the associated Lie ring defined in Section 2.2), then N contains $\mathcal{K}((\boldsymbol{t}^{\boldsymbol{\alpha}})) \cap \mathcal{G}\ell_n^{|\boldsymbol{\alpha}|+2m+1}$, that, by Proposition 5.3, equals $\mathcal{K}\left((\boldsymbol{t}^{\boldsymbol{\alpha}}) \cap \mathfrak{m}^{|\boldsymbol{\alpha}|+2m+2}\right)$.

Example 6.3. In terms of graphs, what happens is the following: suppose that $\boldsymbol{f}$ has restricted 1-support represented by the highest-level black dot on the graphs. Then any element of $\mathcal{G}\ell_n^1$ having support that is a subset of the black bullets set (that is the intersection of the cone with the highest black dot as vertex and the set of dots below a certain horizontal line that depends on m and $\omega(\boldsymbol{f})$) is contained in N.



Proof of Lemma 6.7. By a direct computation, for every $\boldsymbol{\beta}, \boldsymbol{\gamma} \in {\mathbb{N}_0}^n$ and every $j \in \{1, \ldots, n\}$, we see that

$$\left[\left[\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i, \boldsymbol{t}^{\boldsymbol{\beta}}\partial_i\right], \boldsymbol{t}^{\boldsymbol{\gamma}}\partial_j\right] = \left[(\beta_i - \alpha_i)\boldsymbol{t}^{\boldsymbol{\alpha}+j-\boldsymbol{\epsilon}_i}\partial_i, \boldsymbol{t}^{\boldsymbol{\gamma}}\partial_j\right] = \\ \gamma_i\,(\beta_i - \alpha_i)\,\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma}-2\boldsymbol{\epsilon}_i}\partial_j + (\alpha_j + \beta_j - \delta_{ij})(\alpha_i - \beta_i)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\beta}+\boldsymbol{\gamma}-\boldsymbol{\epsilon}_i-\boldsymbol{\epsilon}_j}\partial_i. \quad (6.2)$$

Fix $\boldsymbol{\delta} \in {\mathbb{N}_0}^n$ of weight at least $2m+2$ and let $\boldsymbol{\beta}', \boldsymbol{\gamma}' \in {\mathbb{N}_0}^n$ be such that $\boldsymbol{\beta}' + \boldsymbol{\gamma}' = \boldsymbol{\delta}$ and $|\boldsymbol{\beta}'|, |\boldsymbol{\gamma}'| \geq m+1$. Let $k, h \in \{0,1,2\}$ be constants and choose $\boldsymbol{\beta}, \boldsymbol{\gamma}, \boldsymbol{\lambda}, \boldsymbol{\mu} \in {\mathbb{N}_0}^n$ to be

$$\boldsymbol{\beta} = \boldsymbol{\beta}' + k\boldsymbol{\epsilon}_i, \quad \boldsymbol{\gamma} = \boldsymbol{\gamma}' + (2-k)\boldsymbol{\epsilon}_i, \quad \boldsymbol{\lambda} = \boldsymbol{\beta}' + h\boldsymbol{\epsilon}_i \quad \text{and} \quad \boldsymbol{\mu} = \boldsymbol{\gamma}' + (2-h)\boldsymbol{\epsilon}_i.$$

Applying formula (6.2), we obtain (note that $\beta_j = \beta'_j = \lambda_j$)

$$\left[\left[\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i, \boldsymbol{t}^{\boldsymbol{\beta}}\partial_i\right], \boldsymbol{t}^{\boldsymbol{\gamma}}\partial_j\right] = (\beta'_i + k - \alpha_i)\left((\gamma'_i + 2 - k)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}}\partial_j - (\alpha_j + \beta'_j - \delta_{ij})\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}+\boldsymbol{\epsilon}_i-\boldsymbol{\epsilon}_j}\partial_i\right) \quad \text{and}$$
$$\left[\left[\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i, \boldsymbol{t}^{\boldsymbol{\lambda}}\partial_i\right], \boldsymbol{t}^{\boldsymbol{\mu}}\partial_j\right] = (\beta'_i + h - \alpha_i)\left((\gamma'_i + 2 - h)\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}}\partial_j - (\alpha_j + \beta'_j - \delta_{ij})\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}+\boldsymbol{\epsilon}_i-\boldsymbol{\epsilon}_j}\partial_i\right).$$

Thus, choosing h such that $(\beta'_i + h - \alpha_i)$ is invertible in $\mathbb{F}_q$ and denoting by c its inverse, we have

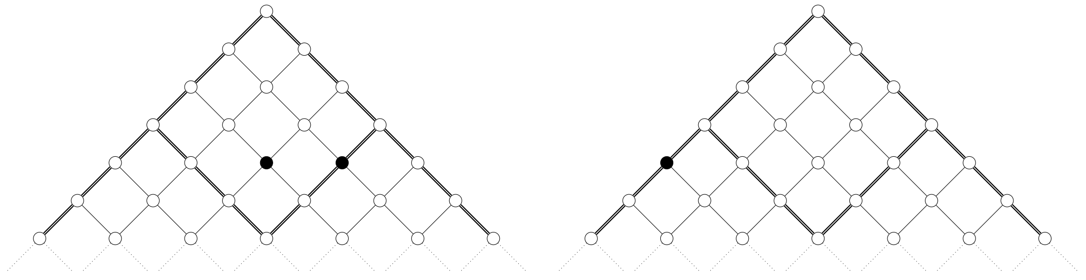
$$c(\beta'_i + k - \alpha_i)\left[\left[\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i, \boldsymbol{t}^{\boldsymbol{\lambda}}\partial_i\right], \boldsymbol{t}^{\boldsymbol{\mu}}\partial_j\right] - \left[\left[\boldsymbol{t}^{\boldsymbol{\alpha}}\partial_i, \boldsymbol{t}^{\boldsymbol{\beta}}\partial_i\right], \boldsymbol{t}^{\boldsymbol{\gamma}}\partial_j\right] = (\beta'_i + k - \alpha_i)\,(h-k)\,\boldsymbol{t}^{\boldsymbol{\alpha}+\boldsymbol{\delta}}\partial_i,$$

where the coefficient $(\beta'_i + k - \alpha_i)(h-k)$ is a polynomial of degree 2 with respect to k. As $p > 2$, such a polynomial is not equivalent to zero modulo p for at least one evaluation of k in $\{0,1,2\}$. Thus the claim easily follows by linearity of Lie brackets. □

Second stage

Lemma 6.8. *Assume $\boldsymbol{f}$ is in $\mathsf{D}\left(s,\ p^2\boldsymbol{\chi}\right)$ for some $s \in \mathbb{N}$ and some $\boldsymbol{\chi} \in {\mathbb{N}_0}^n$. Then, for every $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$ such that $p^{s+2}\lfloor|\boldsymbol{\beta}|/2\rfloor > m$, there exists $\boldsymbol{g} \in N$ such that $\mathsf{A}\left(0,\ (p-1)\mathbf{1},\ \boldsymbol{g},\ 1\right)$ is not empty and $\boldsymbol{g} \in \mathsf{D}\left(s+2,\ \boldsymbol{\chi}+\boldsymbol{\beta}\right)$.*

Example 6.4. The graphical meaning of this lemma is that we can always assume that the restricted 1-support of $\boldsymbol{f}$ in N has a point in the lowest corner of a p-cell, such as the following



where the crucial point is the middle black dot in the left graph.

Proof. First we slightly change our hypothesis, possibly allowing $\boldsymbol{f}$ to be in $\mathsf{D}\,(s+1,\ p\boldsymbol{\chi})$ for some $\boldsymbol{\chi}$ and assuming that there exists $(\boldsymbol{\gamma}, i)$ — where $\boldsymbol{\gamma} = (\gamma_i)_{i=1}^n$ — in the restricted 1-support of $\boldsymbol{f}$ such that $\gamma_{\tilde{j}} \not\equiv_p 0$ for some $\tilde{j} \in \{1,\dots,n\} \setminus \{i\}$. Without loss of generality we may assume $\tilde{j} = 1$. So let $\boldsymbol{\beta}_1 \in {\mathbb{N}_0}^n$ be such that $p^{s+2}|\boldsymbol{\beta}_1| > m$ and define $\boldsymbol{\lambda}$ and $\boldsymbol{\nu} \in {\mathbb{N}_0}^n$ to be $\sum_{j=1}^n (p-1-x_j)\boldsymbol{\epsilon}_j$ and $\boldsymbol{\lambda} + p^{s+2}\boldsymbol{\beta}_1 + \boldsymbol{\epsilon}_1$ respectively, where each x_j is the minimal non-negative integer in the same residue class of γ_j modulo p. Then, the commutator $\boldsymbol{g} = (t_j + g_j)_{j=1}^n$ of $\boldsymbol{t}^{\boldsymbol{\nu}}\boldsymbol{E}_1$ and $\boldsymbol{f}$ is equivalent, by formula (2.2), to $\boldsymbol{t} + \sum_{j=1}^n f_j(\partial_j \boldsymbol{t}^{\boldsymbol{\nu}})\boldsymbol{E}_1 - \boldsymbol{t}^{\boldsymbol{\nu}}\partial_1 \boldsymbol{f}'$ modulo $\mathscr{M}^{\omega(\boldsymbol{f})+|\boldsymbol{\nu}|}$. In particular $g_i = -\boldsymbol{t}^{\boldsymbol{\nu}}\partial_1 f_i$ and thus in the 1-support of $\boldsymbol{g}$ there is $(\boldsymbol{\gamma} + \boldsymbol{\lambda} + p^{s+2}\boldsymbol{\beta}_1, i)$ which is in $\mathsf{A}\,(0,\ (p-1)\mathbf{1},\ \boldsymbol{g},\ 1)$. Moreover, any $(\boldsymbol{\alpha}, j)$ in the restricted 1-support of $\boldsymbol{f}$ is either of the form $(\boldsymbol{\alpha}' + \boldsymbol{\lambda} + p^{s+2}\boldsymbol{\beta}_1, j)$ — where $(\boldsymbol{\alpha}', j) \in \mathrm{Supp}_1\boldsymbol{f}$ — or of the form $(\boldsymbol{\alpha}' + \boldsymbol{\lambda} + p^{s+2}\boldsymbol{\beta}_1 + \boldsymbol{\epsilon}_1 - \boldsymbol{\epsilon}_k, 1)$ — where $(\boldsymbol{\alpha}', k) \in \mathrm{Supp}_1\boldsymbol{f}$ for some $k \in \{1,\dots,n\}$ such that $\boldsymbol{\lambda} \geq \boldsymbol{\epsilon}_k$. In either case, since $\boldsymbol{\alpha}' - p^{s+2}\boldsymbol{\chi}$ is less than or equal to $(p^{s+1}-1)\mathbf{1}$ because of Lemma 6.3 statement (iv) and $\boldsymbol{\lambda}$ is less than or equal to $(p-1)\mathbf{1}$, we have

$$p^{s+2}\boldsymbol{\chi} \leq \boldsymbol{\alpha} - p^{s+2}\boldsymbol{\beta}_1 \leq p^{s+2}\boldsymbol{\chi} + (p^{s+1}-1)\mathbf{1} + p\mathbf{1} \leq p^{s+2}\boldsymbol{\chi} + (p^{s+2}-1)\mathbf{1},$$

whence $\Psi_{s+2}\,(\boldsymbol{\alpha}) = \boldsymbol{\chi} + \boldsymbol{\beta}_1$ by statements (iv) and (i) of Lemma 6.3.

Now assume that $\boldsymbol{f}$ is in $\mathsf{D}\left(s,\ p^2\boldsymbol{\chi}\right)$ as in the statement of this lemma and that for all $(\boldsymbol{\alpha}, i) \in \mathrm{Supp}_1\boldsymbol{f}$ we have $\alpha_j \equiv_p 0$ for every $j \in \{1,\dots,n\} \setminus \{i\}$. We want to reduce the proof to the previous case. Without loss of generality, assume that the depth of $\boldsymbol{f}$ is equal to the order of f_1. Let k be a positive integer and $\boldsymbol{\beta}_2 \in {\mathbb{N}_0}^n$ be such that $p^{s+2}|\boldsymbol{\beta}_2| > m$. Then the commutator $\boldsymbol{h} = (t_i + h_i)_{i=1}^n$ of $\boldsymbol{t}^{p^{s+2}\boldsymbol{\beta}_2 + k\boldsymbol{\epsilon}_1}\boldsymbol{E}_2$ and $\boldsymbol{f}$ is equivalent to $\boldsymbol{t} + kf_1 t_1^{k-1}\boldsymbol{t}^{p^{s+2}\boldsymbol{\beta}_2}\boldsymbol{E}_2 - t_1^k \boldsymbol{t}^{p^{s+2}\boldsymbol{\beta}_2}\partial_2\boldsymbol{f}$ modulo $\mathscr{M}^{\omega(\boldsymbol{f})+p^{s+2}|\boldsymbol{\beta}_2|+k}$. So $h_2 = t_1^{k-1}\boldsymbol{t}^{p^{s+2}\boldsymbol{\beta}_2}(kf_1 - t_1\partial_2 f_2)$ and for at least one choice of $k \in \{1,2\}$ there exists $(\boldsymbol{\alpha}, 2) \in \mathrm{Supp}_1\boldsymbol{h}$ such that $\alpha_1 \not\equiv_p 0$. Moreover, for every $(\boldsymbol{\alpha}, j) \in \mathrm{Supp}_1\boldsymbol{h}$, the n-tuple $\boldsymbol{\alpha}$ is either of the form $\boldsymbol{\alpha}' + p^{s+2}\boldsymbol{\beta}_2 + (k-1)\boldsymbol{\epsilon}_1$ where $(\boldsymbol{\alpha}', 1) \in \mathrm{Supp}_1\boldsymbol{f}$, or of the form $\boldsymbol{\alpha}' + p^{s+2}\boldsymbol{\beta}_2 + k\boldsymbol{\epsilon}_1 - \boldsymbol{\epsilon}_2$ where $(\boldsymbol{\alpha}', j)$ is a pair in $\mathrm{Supp}_1\boldsymbol{f}$ such that $\boldsymbol{\alpha}' - p\Psi_1\,(\boldsymbol{\alpha}') \geq \boldsymbol{\epsilon}_2$. In any case,

$$p^{s+2}\boldsymbol{\chi} \leq \boldsymbol{\alpha} - p^{s+2}\boldsymbol{\beta}_2 \leq \boldsymbol{\alpha}' + \mathbf{1} + \mathbf{1} \leq p^{s+2}\boldsymbol{\chi} + (p^s+1)\mathbf{1} \leq p^{s+2}\boldsymbol{\chi} + (p^{s+1}-1)\mathbf{1}$$

whence $\psi_{s+1}(\boldsymbol{\alpha}) = p(\boldsymbol{\beta}_2 + \boldsymbol{\chi})$.

So we reduced to the first case and we conclude just noting that, given $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$, there exist $\boldsymbol{\beta}_1$ and $\boldsymbol{\beta}_2$ in ${\mathbb{N}_0}^n$ such that $\boldsymbol{\beta}_1 + \boldsymbol{\beta}_2 = \boldsymbol{\beta}$ and $|\boldsymbol{\beta}_i|p^{s+2} > m$ for $i = 1, 2$ if and only if $p^{s+2}\lfloor|\boldsymbol{\beta}|/2\rfloor > m$. □

Third stage

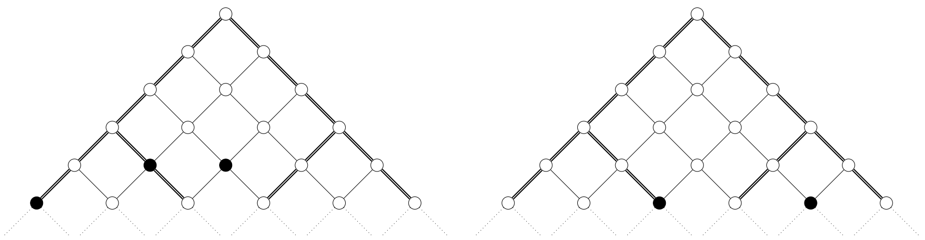
Lemma 6.9. *Let d, l be positive integers. Suppose $\boldsymbol{f}$ is in $\mathsf{S}\,(l,\ d)$ and suppose also that $\omega\,(\boldsymbol{f}) \geq d$. Then, for all $\boldsymbol{\zeta}$ and $\boldsymbol{\beta}$ in ${\mathbb{N}_0}^n$ having the same weight, every $i \in \{1,\dots,n\}$ and every $k \in \{1,\dots,n\}$ such that $\omega\,(\boldsymbol{f}) + 1 = \mathrm{ord}\,(f_k)$, there exists $\boldsymbol{g} = \boldsymbol{t} + \boldsymbol{g}' \in N \cap \mathsf{S}\,(l,\ d)$ such that*

$$\mathrm{Supp}_d(\boldsymbol{g}) = \{(\boldsymbol{\alpha} + p^l\boldsymbol{\zeta} + p^v\boldsymbol{\beta}, i) \mid (\boldsymbol{\alpha}, k) \in \mathrm{Supp}_d(\boldsymbol{f})\}$$

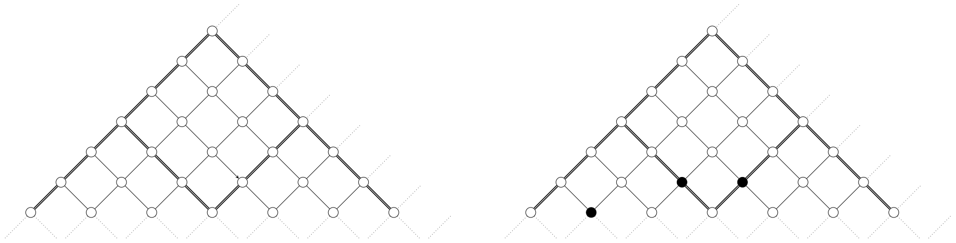
for any $v > l$ such that $p^v \geq d$. In particular $\boldsymbol{g}$ has depth equal to $\omega\,(\boldsymbol{f}) + |\boldsymbol{\zeta}|(p^l + p^v)$ and it is in $\mathsf{S}\,(l,\ d)$.

This lemma is essentially needed to obtain an analogous of Lemma 6.8 when $l > 0$.

Example 6.5. Suppose $\boldsymbol{f}$ has support represented by



where single lines stand for the lattice $p^l{\mathbb{N}_0}^n$ and doubled lines for $p^{l+1}{\mathbb{N}_0}^n$. Then, this lemma implies there exists $\boldsymbol{g} \in N$ whose support is represented by



where the top vertex corresponds to $xt_1^{p^v}$ for some $v, x \in \mathbb{N}$.

Proof. Using induction on $|\boldsymbol{\zeta}|$ it is enough to prove the statement when $|\boldsymbol{\zeta}| = 1$, that is $\boldsymbol{\zeta} = \boldsymbol{\epsilon}_c$ and $\boldsymbol{\beta} = \boldsymbol{\epsilon}_j$ for some $c, j \in \{1, \ldots, n\}$. By hypothesis there exists $\boldsymbol{h} \in (\mathbb{F}_q[\![\boldsymbol{t}]\!])^n$ such that $\boldsymbol{f}' = (\boldsymbol{h})^{p^l} + \boldsymbol{r}$ where $\boldsymbol{r} \in \mathcal{M}^{\omega(\boldsymbol{f})+d+1}$. Then, by formula (1.11), the commutator $\boldsymbol{g} = \boldsymbol{t} + \boldsymbol{g}'$ of $\boldsymbol{t} + t_j^{p^v} t_c^{p^l} t_k \boldsymbol{E}_i$ and $\boldsymbol{f}$ is given by (see also Corollary B.6)

$$\begin{aligned} \boldsymbol{g}' \equiv & \underbrace{f_k t_j^{p^v} t_c^{p^l} \boldsymbol{E}_i}_{(\boldsymbol{g}_1)} + \underbrace{\sum_{|\gamma| \geq p^l} (\boldsymbol{f}')^{\gamma}\, \partial_{\gamma} \left(t_j^{p^v} t_c^{p^l} t_k \right) \boldsymbol{E}_i +}_{\boldsymbol{g}_2} \\ & - \underbrace{\sum_{a>0} (t_j^{p^v} t_c^{p^l} t_i)^{ap^l} (\partial_{a\boldsymbol{\epsilon}_i} \boldsymbol{h})^{p^l}}_{\boldsymbol{g}_3} - \underbrace{\sum_{a>0} (t_j^{p^v} t_c^{p^l} t_i)^{a} (\partial_{\boldsymbol{\epsilon}_i} \boldsymbol{r})}_{\boldsymbol{g}_4} \qquad \bmod \mathfrak{m}^{\omega(\boldsymbol{g})+\min\{\omega(\boldsymbol{f}), p^v+p^l\}+1} \end{aligned}$$

where

$$\begin{aligned} &\operatorname{ord}(\boldsymbol{g}_1) = \omega(\boldsymbol{f}) + 1 + p^v + p^l, \\ &\operatorname{ord}(\boldsymbol{g}_2) \geq p^l(\omega(\boldsymbol{f}) + 1) + p^v + 1 \geq \operatorname{ord}(\boldsymbol{g}_1) + (p^l - 1)\,\omega(\boldsymbol{f}), \\ &\operatorname{ord}(\boldsymbol{g}_3) \geq p^l(p^v + p^l + 1) + \omega(\boldsymbol{f}) + 1 - p^l \geq \operatorname{ord}(\boldsymbol{g}_1) + (p^l - 1)(p^v + p^l), \\ &\operatorname{ord}(\boldsymbol{g}_4) \geq p^v + p^l + 1 + \operatorname{ord}(\boldsymbol{r}) - 1 \geq \operatorname{ord}(\boldsymbol{g}_1) + d. \end{aligned}$$

Hence the claim follows, as $\boldsymbol{g} \equiv \boldsymbol{t} + f_k t_j^{p^v} t_c^{p^l} \boldsymbol{E}_i$ modulo $\mathfrak{m}^{\omega(\boldsymbol{g})+d+1}$. □

Fourth stage

Recall that $\lfloor g \rfloor_r$, for every $g \in \mathbb{F}_q[\![\boldsymbol{t}]\!]$ and every $r \in \mathbb{N}$, denotes the lowest degree representative of the class $g + \mathfrak{m}^{r+1}$. When $\boldsymbol{g} = (g_i)_{i=1}^n \in (\mathbb{F}_q[\![\boldsymbol{t}]\!])^n$, we use the same notation $\lfloor \boldsymbol{g} \rfloor_r$ to denote $(\lfloor g_i \rfloor_r)_{i=1}^n$.

Proposition 6.10. *Fix $\boldsymbol{\zeta} \leq (p-1)\mathbf{1}$ and $\boldsymbol{\beta}$ in ${\mathbb{N}_0}^n$ of weight w, say $\boldsymbol{\zeta} = \sum_{i=1}^{w} \boldsymbol{\epsilon}_{c_i}$ and $\boldsymbol{\beta} = \sum_{i=1}^{w} \boldsymbol{\epsilon}_{j_i}$ for $(c_i)_{i=1}^w, (j_i)_{i=1}^w$ in $\{1, \ldots, n\}^w$. Let v, l, d_0, d_w be non-negative integers. Suppose that* *(i)* $v > l$ *and* $p^v > m$.

(ii) $d_w \geq d_0 + w(p^l - 1)(p^v - 1)$.

(iii) $\boldsymbol{f}$ *is in* $\mathsf{S}\,(l,\ d_w)$ *and* $\omega\,(\boldsymbol{f}) \geq \max\{p^l, d_w\}$.

(iv) $\mathsf{A}\,(l,\ \boldsymbol{\zeta},\ \boldsymbol{f},\ 1)$ *is non-empty, i. e.* $\partial_{p^l \boldsymbol{\epsilon}_{c_w}} \partial_{p^l \boldsymbol{\epsilon}_{c_{w-1}}} \ldots \partial_{p^l \boldsymbol{\epsilon}_{c_1}} \lfloor \boldsymbol{f}' \rfloor_{\mathrm{ord}(\boldsymbol{f}')} \neq 0$.

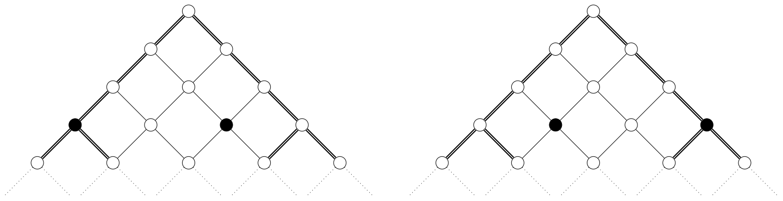
Then there exists $\boldsymbol{g} \in N$ *of depth* $\omega\,(\boldsymbol{f}) + wp^l(p^v - 1)$ *such that*

$$\boldsymbol{g} \equiv \boldsymbol{t} + \left(\sum_{a_1 \ldots a_w} t_{j_w}^{a_w p^v} \partial_{a_w \boldsymbol{\epsilon}_{c_w}} \left(t_{j_{w-1}}^{a_{w-1} p^v} \partial_{a_{w-1} \boldsymbol{\epsilon}_{c_{w-1}}} \left(\ldots t_{j_1}^{a_1 p^v} \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \ldots \right) \right) \right)^{p^l} \mod \mathcal{M}^{\omega(\boldsymbol{g}) + d_0 + 1}$$

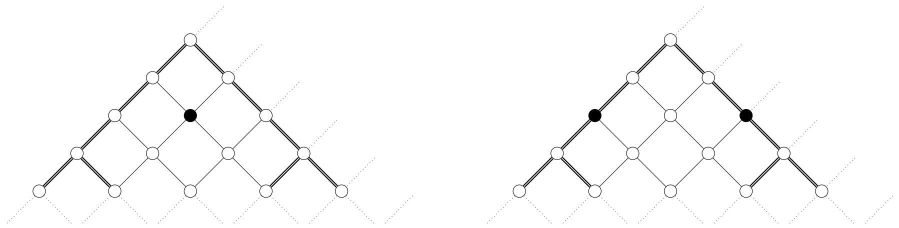
where $\boldsymbol{h}$ *is such that* $\boldsymbol{f} \equiv \boldsymbol{t} + \boldsymbol{h}^{p^l}$ *modulo* $\mathcal{M}^{\omega(\boldsymbol{f}) + d_w + 1}$. *In particular* $\boldsymbol{g}$ *is in* $\mathsf{S}\,(l,\ d_0)$.

This result is somewhat the converse of the previous one. Assume $\boldsymbol{f}$ is in $\mathsf{S}\,(l,\ d_1)$ for some large enough positive integer d_1. While in Lemma 6.9 we said we may move forward the bounded d_1-support of $\boldsymbol{f}$ with respect to the sublattice $p^{l+1}{\mathbb{N}_0}^n$, here we say we can also move backward the d_0-support for some $d_0 \leq d_1$, but in doing so we are losing some points in the 1-support, namely those that "cross double lines" in our representation of supports.

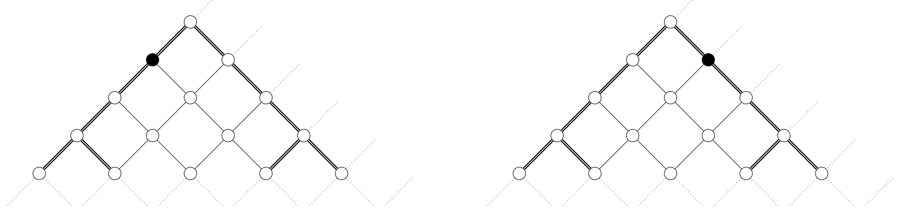
Example 6.6. Suppose $\boldsymbol{f} \in \mathsf{S}\,(l,\ d_1)$, where $d_1 >> 0$, has the following 1-support



where — as usual — single lines represents $p^l{\mathbb{N}_0}^n$ and double lines $p^{l+1}{\mathbb{N}_0}^n$. Then, for example, we can find $\boldsymbol{g} \in \mathsf{S}\,(l,\ d_0) \cap N$ whose 1-support is



if $\boldsymbol{\zeta} = \boldsymbol{\epsilon}_2$ and $\boldsymbol{\beta} = 2p^v\boldsymbol{\epsilon}_1$ or



if $\boldsymbol{\zeta} = 2\boldsymbol{\epsilon}_1$ and $\boldsymbol{\beta} = 2p^v\boldsymbol{\epsilon}_1$, with the usual conventions.

The proof of this result is also by induction. However, since it is more complicated, we split it, starting by proving the base case.

Lemma 6.11. *Let v, l, d_0, d_1 be non-negative integers and let j, c be in $\{1, \dots, n\}$. Suppose that*

(i) $v > l$ and $p^v > m$.

(ii) $d_1 \geq d_0 + (p^l - 1)(p^v - 1)$.

(iii) $\boldsymbol{f}$ is in $\mathsf{S}(l,\ d_1)$ and $\omega(\boldsymbol{f}) \geq \max\{p^l, d_0\}$.

(iv) $\mathsf{A}(l,\ \boldsymbol{\epsilon}_c,\ \boldsymbol{f},\ 1)$ is non-empty, i. e. $\partial_{p^l\boldsymbol{\epsilon}_c}\lfloor \boldsymbol{f}' \rfloor_{\mathrm{ord}(f')} \neq 0$.

Then there exists $\boldsymbol{g} \in N$ of depth $\omega(\boldsymbol{f}) + p^l(p^v - 1)$ such that

$$\boldsymbol{g} \equiv \boldsymbol{t} + \left(\sum_{a>0} t_j^{ap^v} \partial_{a\boldsymbol{\epsilon}_c} \boldsymbol{h} \right)^{p^l} \mod \mathcal{M}^{\omega(\boldsymbol{g})+d_0+1}$$

where $\boldsymbol{f} \equiv \boldsymbol{t} + \boldsymbol{h}^{p^l}$ modulo $\mathcal{M}^{\omega(\boldsymbol{f})+d_1+1}$. In particular $\boldsymbol{g}$ is in $\mathsf{S}(l,\ d_0)$.

Proof. By hypothesis there exists $\boldsymbol{r}$ in $(\mathbb{F}_q[\![\boldsymbol{t}]\!])^n$ of order at least $\omega(\boldsymbol{f})+d_1+1$ such that $\boldsymbol{f}' = \boldsymbol{h}^{p^l} + \boldsymbol{r}$ where $\boldsymbol{h}, \boldsymbol{r} \in (\mathbb{F}_q[\![\boldsymbol{t}]\!])^n$. By equation (1.7) we have

$$(\boldsymbol{t} + t_j^{p^v}\boldsymbol{E}_c) \circ \boldsymbol{f} = \boldsymbol{t} + t_j^{p^v}\boldsymbol{E}_c + \boldsymbol{h}^{p^l} + \boldsymbol{r} + f_j^{p^v}\boldsymbol{E}_c$$

and therefore, applying equation (1.11) to compute the commutator $\boldsymbol{g} = \boldsymbol{t}+\boldsymbol{g}'$ of $\boldsymbol{f}$ and $\boldsymbol{t} + t_j^{p^v}\boldsymbol{E}_c$, we obtain (see also Lemma B.6)

$$\begin{aligned}
\boldsymbol{g}' =& \sum_{a>0} t_j^{ap^v} \partial_{a\boldsymbol{\epsilon}_c} \boldsymbol{h}^{p^l} + \sum_{a>0} t_j^{ap^v} \partial_{a\boldsymbol{\epsilon}_c} \boldsymbol{r} - (f_j)^{p^v}\boldsymbol{E}_c - \sum_{\boldsymbol{\alpha}>\boldsymbol{0}} (\boldsymbol{g}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \left(t_j^{p^v}\boldsymbol{E}_c + \boldsymbol{h}^{p^l} + \boldsymbol{r} + f_j^{p^v}\boldsymbol{E}_c \right) \\
=& \underbrace{\left(\sum_{a>0} t_j^{ap^v} \partial_{a\boldsymbol{\epsilon}_c} \boldsymbol{h} \right)^{p^l}}_{\boldsymbol{g}_1} - \underbrace{\left(f_j^{p^{v-l}} \boldsymbol{E}_c \right)^{p^l}}_{\boldsymbol{g}_2} - \underbrace{\left(\sum_{\boldsymbol{\alpha}>\boldsymbol{0}} (\boldsymbol{g}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} (t_j\boldsymbol{E}_c + f_j\boldsymbol{E}_c) \right)^{p^v}}_{\boldsymbol{g}_3} - \underbrace{\left(\sum_{\boldsymbol{\alpha}>\boldsymbol{0}} (\boldsymbol{g}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \boldsymbol{h} \right)^{p^l}}_{\boldsymbol{g}_4} \\
&+ \underbrace{\sum_{a>0} (t_j)^{ap^v} \partial_{a\boldsymbol{\epsilon}_c} \boldsymbol{r}}_{\boldsymbol{g}_5} - \underbrace{\sum_{\boldsymbol{\alpha}>\boldsymbol{0}} (\boldsymbol{g}')^{\boldsymbol{\alpha}} \partial_{\boldsymbol{\alpha}} \boldsymbol{r}}_{\boldsymbol{g}_6}
\end{aligned}$$

where

$$\begin{aligned}
&\mathrm{ord}(\boldsymbol{g}_1) = p^l(p^v + \mathrm{ord}(\boldsymbol{h}) - 1) = p^{l+v} + \omega(\boldsymbol{f}) + 1 - p^l = p^l(p^v - 1) + \omega(\boldsymbol{f}) + 1 \\
&\mathrm{ord}(\boldsymbol{g}_2) \geq p^v \mathrm{ord}(\boldsymbol{f}) \geq p^v(\omega(\boldsymbol{f}) + 1) \geq (p^v - 1)(\omega(\boldsymbol{f}) + 1 - p^l) + \mathrm{ord}(\boldsymbol{g}_1) \\
&\mathrm{ord}(\boldsymbol{g}_3) \geq p^v\,\omega(\boldsymbol{g}) > \omega(\boldsymbol{g}) + \omega(\boldsymbol{f}) \\
&\mathrm{ord}(\boldsymbol{g}_4) \geq p^l\,\omega(\boldsymbol{g}) + p^l \mathrm{ord}(\boldsymbol{h}) \geq \omega(\boldsymbol{g}) + \omega(\boldsymbol{f}) + 1 \\
&\mathrm{ord}(\boldsymbol{g}_5) \geq p^v + \omega(\boldsymbol{f}) + d_1 = \mathrm{ord}(\boldsymbol{g}_1) + d_1 - (p^v - 1)(p^l - 1) \geq \mathrm{ord}(\boldsymbol{g}_1) + d_0 \\
&\mathrm{ord}(\boldsymbol{g}_6) \geq \omega(\boldsymbol{g}) + \omega(\boldsymbol{f}) + d_1 > \omega(\boldsymbol{g}) + \omega(\boldsymbol{f})
\end{aligned}$$

that is $\boldsymbol{g}' \equiv \boldsymbol{g}_1 + \boldsymbol{g}_2 + \boldsymbol{g}_5$ modulo $\mathscr{M}^{\omega(\boldsymbol{g})+\omega(\boldsymbol{f})+1}$. Moreover

$$\begin{aligned}(p^v-1)(\omega(\boldsymbol{f})+1-p^l) = (p^v-2)\,\omega(\boldsymbol{f}) - (p^l-1)(p^v-1) + \omega(\boldsymbol{f}) \geq \\ \geq (p^v-2)p^l - (p^l-1)(p^v-1) + \omega(\boldsymbol{f}) \geq p^v - p^l - 1 + \omega(\boldsymbol{f}) > \omega(\boldsymbol{f})\end{aligned}$$

and therefore $\boldsymbol{g}'$ is equivalent to $\boldsymbol{g}_1 + \boldsymbol{g}_5$ modulo $\mathscr{M}^{\omega(\boldsymbol{g})+\omega(\boldsymbol{f})+1}$ and to $\boldsymbol{g}_1$ modulo $\mathscr{M}^{\omega(\boldsymbol{g})+d_0+1}$. □

We are now able to approach the actual proof of Proposition 6.10.

Proof of Proposition 6.10. As already mentioned, we proceed by induction on w, the base case being an application of the previous lemma. So let $\boldsymbol{\zeta}'$ and $\boldsymbol{\beta}'$ equal $\sum_{i=1}^{w-1} \boldsymbol{\epsilon}_{c_i}$ and $\sum_{i=1}^{w-1} \boldsymbol{\epsilon}_{j_i}$ respectively and let d_1 be equal to $d_0 + (p^v-1)(p^l-1)$. Then by inductive hypothesis there exists $\boldsymbol{g}_1 = (\boldsymbol{t} + \boldsymbol{g}_1') \in N$ of weight $\omega(\boldsymbol{f}) + (w-1)p^l(p^v-1)$ such that

$$\boldsymbol{g}_1 \equiv \boldsymbol{t} + \left(\sum_{a_1 \dots a_{w-1}} t_{j_{w-1}}^{a_{w-1}p^v} \partial_{a_{w-1}\boldsymbol{\epsilon}_{c_{w-1}}} \left(\dots t_{j_1}^{a_1 p^v} \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \dots \right) \right)^{p^l} \qquad \bmod \mathscr{M}^{\omega(\boldsymbol{g})+d_1+1}.$$

Note that when $a_{w-1}, a_{w-2}, \dots, a_1$ are all equal to 1, we have

$$t_{j_{w-1}}^{a_{w-1}p^v} \partial_{a_{w-1}\boldsymbol{\epsilon}_{c_{w-1}}} \left(\dots t_{j_1}^{a_1 p^v} \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \dots \right) = \boldsymbol{t}^{p^v \boldsymbol{\beta}'} \partial_{\boldsymbol{\epsilon}_{c_{w-1}}} \partial_{\boldsymbol{\epsilon}_{c_{w-2}}} \dots \partial_{\boldsymbol{\epsilon}_{c_1}} \boldsymbol{h}$$

(see Lemma B.8) and when there exists at least one a_i that is greater than 1, then

$$\begin{aligned}\operatorname{ord}\left(\left(t_{j_{w-1}}^{a_{w-1}p^v} \partial_{a_{w-1}\boldsymbol{\epsilon}_{c_{w-1}}} \left(\dots t_{j_1}^{a_1 p^v} \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \dots \right) \right)^{p^l} \right) \geq \\ \geq p^l((p^v-1)w + \operatorname{ord}(\boldsymbol{h})) \geq p^l(p^v-1)w + \omega(\boldsymbol{f}) + 1 \geq \\ \geq \omega(\boldsymbol{g}_1) + p^l(p^v-1)\end{aligned}$$

that is to say $\boldsymbol{g}_1'$ is equivalent to $\left(\boldsymbol{t}^{p^v \boldsymbol{\beta}'} \partial_{\boldsymbol{\epsilon}_{c_1}} \dots \partial_{\boldsymbol{\epsilon}_{c_{w-1}}} h \right)^{p^l}$ modulo $\mathscr{M}^{\omega(\boldsymbol{g})+2}$. In particular $\partial_{p^l \boldsymbol{\epsilon}_{c_w}} \lfloor \boldsymbol{g}_1' \rfloor_{\operatorname{ord}(\boldsymbol{g}_1')}$ equals $\boldsymbol{t}^{p^{v+l} \boldsymbol{\beta}'} \partial_{p^l \boldsymbol{\epsilon}_{c_w}} \dots \partial_{p^l \boldsymbol{\epsilon}_{c_1}} \lfloor \boldsymbol{f}' \rfloor_{\operatorname{ord}(\boldsymbol{f}')}$ and it is not zero by hypothesis. Thus we can apply the previous lemma, obtaining the desired result. □

Corollary 6.12. *In the same hypothesis and notations of Proposition 6.10 and assuming also that $\boldsymbol{\zeta} = (p-1)\mathbf{1}$ and $p^l(p^v-1)(p-1) \geq d_0$, the resulting $\boldsymbol{g} \in N$ has d_0-support equal to*

$$\operatorname{Supp}_{d_0} \boldsymbol{g} = \left\{ \left(p^{l+1} \Psi_{l+1}(\boldsymbol{\alpha}) + p^{v+l} \boldsymbol{\beta}, u \right) \mid (\boldsymbol{\alpha}, u) \in \mathsf{A}(l,\ (p-1)\mathbf{1},\ \boldsymbol{f},\ d_0) \right\}$$

and in particular is in $\mathsf{S}(l+1,\ d_0)$. Moreover, if $\boldsymbol{f}$ is in $\mathsf{D}(s,\ \boldsymbol{\chi})$ for some $\boldsymbol{\chi} \in {\mathbb{N}_0}^n$ and $l < s \leq v$, then $\boldsymbol{g}$ is in $\mathsf{D}\left(s,\ \boldsymbol{\chi} + p^{v+l-s}\boldsymbol{\beta}\right)$.

Proof. First of all observe that, by Lemma B.8, whenever $a_i < p$ for every $i \in \{1, \dots, w\}$, we have

$$\begin{aligned}t_{j_w}^{a_w p^v} \partial_{a_w \boldsymbol{\epsilon}_{c_w}} \left(t_{j_{w-1}}^{a_{w-1}p^v} \partial_{a_{w-1}\boldsymbol{\epsilon}_{c_{w-1}}} \left(\dots t_{j_1}^{a_1 p^v} \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \dots \right) \right) = \\ = \boldsymbol{t}^{p^v \sum_{i=1}^{w} a_i \boldsymbol{\epsilon}_{j_w}} \partial_{a_w \boldsymbol{\epsilon}_{c_w}} \left(\partial_{a_{w-1}\boldsymbol{\epsilon}_{c_{w-1}}} \left(\dots \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \dots \right) \right)\end{aligned}$$

that, by Corollary B.13, is 0 unless $a_1 = a_2 = \ldots = a_w = 1$, since $\sum_{i=1}^{w} \boldsymbol{\epsilon}_{j_i} = (p-1)\mathbf{1}$. On the other hand, if there exists at least one $i \in \{1, \ldots, w\}$ such that $a_i = p$, then the order of

$$\left(t_{j_w}^{a_w p^v} \partial_{a_w \boldsymbol{\epsilon}_{c_w}} \left(t_{j_{w-1}}^{a_{w-1} p^v} \partial_{a_{w-1} \boldsymbol{\epsilon}_{c_{w-1}}} \left(\ldots t_{j_1}^{a_1 p^v} \partial_{a_1 \boldsymbol{\epsilon}_{c_1}} \boldsymbol{h} \ldots\right)\right)\right)^{p^l}$$

is at least

$$\begin{aligned} p^l(\operatorname{ord}(\boldsymbol{h}) + p(p^v-1) + (w-1)(p^v-1)) = \\ = \omega(\boldsymbol{f}) + pp^l(p^v-1) + (w-1)p^l(p^v-1) + 1 = \omega(\boldsymbol{g}) + p^l(p^v-1)(p-1) + 1 \geq \\ \geq \omega(\boldsymbol{g}) + d_0 + 1.. \end{aligned}$$

It follows that $\boldsymbol{g}$ is equivalent to $\boldsymbol{t} + \left(\boldsymbol{t}^{p^v \boldsymbol{\beta}} \partial_{\boldsymbol{\epsilon}_{j_w}} \partial_{\boldsymbol{\epsilon}_{j_{w-1}}} \ldots \partial_{\boldsymbol{\epsilon}_{j_1}} \boldsymbol{h}\right)^{p^l}$ modulo $\mathcal{M}^{\omega(\boldsymbol{g})+d_0+1}$. Furthermore, by Remark 6.6, we have that

$$\operatorname{Supp}_{d_0}\boldsymbol{g} = \{\left(\boldsymbol{\alpha} + p^l\left(p^v\boldsymbol{\beta} - (p-1)\mathbf{1}\right), u\right) \mid (\boldsymbol{\alpha}, u) \in \mathsf{A}\left(l,\ (p-1)\mathbf{1},\ \boldsymbol{f},\ d_0\right)\}$$

and by Corollary 6.5, we have that $(\boldsymbol{\alpha}, u)$ is in $\mathsf{A}\left(l,\ (p-1)\mathbf{1},\ \boldsymbol{f},\ d_0\right)$ if and only if it equals $\Psi_{l+1}(\boldsymbol{\alpha}) + p^l(p-1)\mathbf{1}$. Therefore

$$\operatorname{Supp}_{d_0}\boldsymbol{g} = \{\left(p^{l+1}\Psi_{l+1}(\boldsymbol{\alpha}) + p^{v+l}\boldsymbol{\beta}, u\right) \mid (\boldsymbol{\alpha}, u) \in \mathsf{A}\left(l,\ (p-1)\mathbf{1},\ \boldsymbol{f},\ d_0\right)\}$$

that is $\boldsymbol{g}$ is in $\mathsf{S}\left(l+1,\ d_0\right)$. Moreover, for every $\left(p^{l+1}\Psi_{l+1}(\boldsymbol{\alpha}) + p^{v+l}\boldsymbol{\beta}, u\right) \in \operatorname{Supp}_{d_0}\boldsymbol{g}$, we have $\Psi_s\left(p^{l+1}\Psi_{l+1}(\boldsymbol{\alpha}) + p^{v+l}\boldsymbol{\beta}\right) = p^{v+l-s}\boldsymbol{\beta} + \Psi_s(\boldsymbol{\alpha})$ by Lemma 6.3, whence we obtain the claim. □

6.3 Actual proof

First of all we may mesh up stages 3 and 4 in the following statement.

Proposition 6.13. *Let l, s and d_0 be positive integers and let $v > s$ be a positive integer such that $p^l(p^v-1)(p-1) \geq d_0$ and $p^v > m$. Define $d := d_0 + n(p-1)(p^l-1)(p^v-1)$. Assume $\boldsymbol{f}$ is such that*

(i) it is in $\mathsf{S}\left(l,\ d\right)$;

(ii) it is in $\mathsf{D}\left(s,\ \boldsymbol{\chi}\right)$ for some $\boldsymbol{\chi} \in \mathbb{N}_0{}^n$;

(iii) its depth is greater than or equal to both p^l and d.

Fix $(\boldsymbol{\gamma}, k) \in \operatorname{Supp}_1\boldsymbol{f}$ and let $\boldsymbol{v}$ be $\Psi_l(\boldsymbol{\gamma}) - p\Psi_{l+1}(\boldsymbol{\gamma})$ and $\boldsymbol{\zeta}$ be $(p-1)\mathbf{1} - \boldsymbol{v}$. Then for every $\boldsymbol{\beta}$ and $\boldsymbol{\eta}$ in $\mathbb{N}_0{}^n$ of weight $|\boldsymbol{\zeta}|$ and $n(p-1)$ respectively, and every $i \in \{1, \ldots, n\}$, there exists $\boldsymbol{g} \in N$ whose restricted d_0-support is

$$\begin{aligned} \operatorname{Supp}_{d_0}\boldsymbol{g} = \{\left(p^{l+1}\Psi_{l+1}(\boldsymbol{\alpha}) + p^v\boldsymbol{\beta} + p^{v+l}\boldsymbol{\eta}, i\right) \in \mathbb{N}_0{}^n \times \{1, \ldots, n\} \mid \\ (\boldsymbol{\alpha}, k) \in \operatorname{Supp}_{d_0}\boldsymbol{f} \text{ s. t. } \Psi_l(\boldsymbol{\alpha}) - p\Psi_{l+1}(\boldsymbol{\alpha}) = \boldsymbol{v}\}. \end{aligned}$$

In particular it is in $\mathsf{S}\left(l+1,\ d_0\right)$ and $\mathsf{D}\left(s,\ \boldsymbol{\chi} + p^{v-s}\boldsymbol{\beta} + p^{v+l-s}\boldsymbol{\eta}\right)$.

Proof. By Lemma 6.9 there exists $\boldsymbol{g}_1 \in N$ whose restricted d-support is

$$\mathrm{Supp}_d(\boldsymbol{g}_1) = \{(\boldsymbol{\alpha} + p^l\boldsymbol{\zeta} + p^v\boldsymbol{\beta}, i) \mid (\boldsymbol{\alpha}, k) \in \mathrm{Supp}_d(\boldsymbol{f})\}.$$

Let $(\boldsymbol{\alpha} + p^l\boldsymbol{\zeta} + p^v\boldsymbol{\beta}, i)$ be in $\mathrm{Supp}_d(\boldsymbol{g}_1)$ for some $(\boldsymbol{\alpha}, k) \in \mathrm{Supp}_d\boldsymbol{f}$ and let $\boldsymbol{\delta} \in {\mathbb{N}_0}^n$ be such that $\boldsymbol{\alpha} = p^{l+1}\varPsi_{l+1}(\boldsymbol{\alpha}) + p^l\boldsymbol{\delta}$, in particular $\boldsymbol{\delta} \leq (p-1)\mathbf{1}$. By Corollary 6.5 we have that $(\boldsymbol{\alpha}+p^l\boldsymbol{\zeta}+p^v\boldsymbol{\beta}, i)$ is in $\mathsf{A}(l,\ (p-1)\mathbf{1},\ \boldsymbol{g}_0,\ d_0)$ if and only if $p^l\boldsymbol{\delta} + p^l\boldsymbol{\zeta} = p^{l+1}\varPsi_{l+1}(\boldsymbol{\delta}+\boldsymbol{\zeta}) + p^l(p-1)\mathbf{1}$. This last condition is equivalent to $\boldsymbol{\zeta}+\boldsymbol{\delta} = (p-1)\mathbf{1}$, since both $\boldsymbol{\zeta}$ and $\boldsymbol{\delta}$ are less than or equal to $(p-1)\mathbf{1}$ and therefore their sum can not contain $p\boldsymbol{\epsilon}_j + (p-1)\boldsymbol{\epsilon}_j$ for any $j \in \{1, \ldots, n\}$. Thus $(\boldsymbol{\alpha}+p^l\boldsymbol{\zeta}+p^v\boldsymbol{\beta}, i)$ is in $\mathsf{A}(l,\ (p-1)\mathbf{1},\ \boldsymbol{g}_0,\ d_0)$ if and only if $\boldsymbol{\delta}$ — that coincides with $\varPsi_l(\boldsymbol{\alpha}) - p\varPsi_{l+1}(\boldsymbol{\alpha})$ — equals $\boldsymbol{v}$. In particular $(\boldsymbol{\gamma} + p^l\boldsymbol{\zeta} + p^v\boldsymbol{\beta}, i)$ is in $\mathsf{A}(l,\ (p-1)\mathbf{1},\ \boldsymbol{g}_0,\ 1)$ that is not empty, thus we may apply Corollary 6.12 in order to find $\boldsymbol{g} \in N$ such that

$$\mathrm{Supp}_{d_0}\boldsymbol{g} = \{\left(p^{l+1}\varPsi_{l+1}\left(\boldsymbol{\alpha} + p^l\boldsymbol{\zeta} + p^v\boldsymbol{\beta}\right) + p^{v+l}\boldsymbol{\eta}, i\right) \mid \\ (\boldsymbol{\alpha} + p^l\boldsymbol{\zeta} + p^v\boldsymbol{\beta}, i) \in \mathsf{A}(l,\ (p-1)\mathbf{1},\ \boldsymbol{g}_1,\ d_0)\}$$

and the statement follows from the just given characterization of elements $(\boldsymbol{\alpha}+p^l\boldsymbol{\zeta}+p^v\boldsymbol{\beta}, i)$ that are in $\mathsf{A}(l,\ (p-1)\mathbf{1},\ \boldsymbol{g}_1,\ d_0)$. □

Now we may want to proceed by iteratively applying this proposition. In order to do so, we need some control over appearing parameters, so we construct two related sequences of coefficients. Fix two positive integers s and d_s. For every non-negative integer l less than s, we define

$$\begin{cases} v_l := \min\{v \in \mathbb{N} \mid v \geq s,\ p^v > m \text{ and } p^l(p^v-1)(p-1) \geq d_{l+1}\}, \\ d_l := d_{l+1} + n(p-1)(p^l-1)(p^{v_l}-1). \end{cases} \tag{6.3}$$

These two sequences clearly depend on the choices of s and d_s. However, since these two parameters will be always fixed, we avoid referring to them in our notation.

Proposition 6.14. *Let l_1 and l_2 be positive integers such that $1 \leq l_1 < l_2 \leq s$. Assume that:*

(i) $\boldsymbol{f}$ is in $\mathsf{S}(l_1,\ d_{l_1})$;

(ii) $\boldsymbol{f}$ is in $\mathsf{D}(s,\ \boldsymbol{\chi})$ for some $\boldsymbol{\chi} \in {\mathbb{N}_0}^n$;

(iii) the depth of $\boldsymbol{f}$ is greater than d_{l_1} (that implies $\omega(\boldsymbol{f}) \geq p^{l_2}$).

Fix $(\boldsymbol{\gamma}, k) \in \mathrm{Supp}_1\boldsymbol{f}$ and, for every $l_1 \leq l < l_2$, define $\boldsymbol{v}_l$ to be $\varPsi_l(\boldsymbol{\gamma}) - p\varPsi_{l+1}(\boldsymbol{\gamma})$ and let $\boldsymbol{\beta}_l$ and $\boldsymbol{\eta}_l$ be any n-tuples in ${\mathbb{N}_0}^n$ of weight $(p-1)n - |\boldsymbol{v}_l|$ and $n(p-1)$ respectively. Then, for every $i \in \{1, \ldots, n\}$, there exists $\boldsymbol{g}$ in N such that

$$\mathrm{Supp}_{d_{l_2}}\boldsymbol{g} = \left\{ \left(p^{l_2}\varPsi_{l_2}(\boldsymbol{\alpha}) + \sum_{l=l_1}^{l_2-1}\left(p^{v_l}\boldsymbol{\beta}_l + p^{v_l+l}\boldsymbol{\eta}_l\right), i \right) \in {\mathbb{N}_0}^n \times \{1, \ldots, n\} \mid \\ (\boldsymbol{\alpha}, k) \in \mathrm{Supp}_{d_{l_2}}\boldsymbol{f} \text{ s. t. } \varPsi_l(\boldsymbol{\alpha}) - p\varPsi_{l+1}(\boldsymbol{\alpha}) = \boldsymbol{v}_l \text{ for every } l_1 \leq l < l_2 \right\}.$$

In particular $\boldsymbol{g}$ is in $\mathsf{S}(l_2,\ d_{l_2})$ and in $\mathsf{D}(s,\ \boldsymbol{\chi}')$ where $\boldsymbol{\chi}'$ is $\boldsymbol{\chi} + \sum_{l=l_1}^{l_2-1}\left(p^{v_l-s}\boldsymbol{\beta}_l + p^{v_l+l-s}\boldsymbol{\eta}_l\right)$.

Proof. This is achieved by a simple induction on $l_2 - l_1$, using the previous proposition for the base case. Let $\boldsymbol{g}_1$ be the element in N obtained by inductive hypothesis on $l_2 - 1$ and l_1, that is $\boldsymbol{g}_1$ such that

$$\mathrm{Supp}_{d_{l_2-1}}\boldsymbol{g}_1 = \left\{ \left(p^{l_2-1}\Psi_{l_2-1}\left(\boldsymbol{\alpha}\right) + \sum_{l=l_1}^{l_2-2} \left(p^{v_l}\boldsymbol{\beta}_l + p^{v_l+l}\boldsymbol{\eta}_l \right), i \right) \in {\mathbb{N}_0}^n \times \{1, \ldots, n\} \mid \right.$$

$$\left. \left(\boldsymbol{\alpha}, k\right) \in \mathrm{Supp}_{d_{l_2-1}}\boldsymbol{f} \text{ s. t. } \Psi_l\left(\boldsymbol{\alpha}\right) - p\Psi_{l+1}\left(\boldsymbol{\alpha}\right) = \boldsymbol{v}_l \text{ for every } l_1 \leq l < l_2 - 1 \right\}$$

and in particular $\boldsymbol{g}_1$ is in $\mathsf{S}\left(l_2 - 1,\ d_{l_2-1}\right)$ and in $\mathsf{D}\left(s,\ \boldsymbol{\chi} + \sum_{l=l_1}^{l_2-2}\left(p^{v_l-s}\boldsymbol{\beta}_l + p^{v_l+l-s}\boldsymbol{\eta}_l\right)\right)$. Since d_{l_2-1} equals $d_{l_2} + n(p-1)(p^{v_{l_2-1}} - 1)(p^{l_2-1} - 1)$ by definition, we may apply Proposition 6.13 and — in order to obtain the desired result — it suffices to note that, by Lemma 6.3, (i)

$$p^{l_2}\Psi_{l_2}\left(p^{l_2-1}\Psi_{l_2-1}\left(\boldsymbol{\alpha}\right) + \sum_{l=l_1}^{l_2-2}\left(p^{v_l}\boldsymbol{\beta}_l + p^{v_l+l}\boldsymbol{\eta}_l\right) \right) =$$

$$= p^{l_2}\Psi_{l_2}\left(p^{l_2-1}\Psi_{l_2-1}\left(\boldsymbol{\alpha}\right)\right) + \sum_{l=l_1}^{l_2-2}\left(p^{v_l}\boldsymbol{\beta}_l + p^{v_l+l}\boldsymbol{\eta}_l\right)$$

where $\Psi_{l_2}\left(p^{l_2-1}\Psi_{l_2-1}\left(\boldsymbol{\alpha}\right)\right) = \Psi_{l_2}\left(\boldsymbol{\alpha}\right)$ by statements (iv) and (v) of Lemma 6.3. □

Remark 6.15. We stress the fact that all $\boldsymbol{\beta}_l$ and $\boldsymbol{\eta}_l$ depend only on the choice of $(\boldsymbol{\gamma}, k) \in \mathrm{Supp}_1\boldsymbol{f}$.

Now we can finally sum up all previous results to obtain our main theorem.

Proof of Theorem 0.2. Let $(\boldsymbol{\alpha}, i)$ be in $\mathrm{Supp}_1\boldsymbol{f}$. Then the weight of $\boldsymbol{\alpha}$ equals $\omega\left(\boldsymbol{f}\right) + 1$ and so it is clear that $\boldsymbol{\alpha} \leq \left(\omega\left(\boldsymbol{f}\right) + 1\right)\mathbf{1}$. This means that $\boldsymbol{f}$ is in $\mathsf{D}\left(s-2,\ 0\right)$ for any integer s such that $p^{s-2} > \omega\left(\boldsymbol{f}\right) + 1$. Fix $j \in \{1, \ldots, n\}$ and consider the sequence of $\{d_i \mid s \geq i \geq 0\}$ defined in (6.3) starting from some $d_s > 0$.

Applying Lemma 6.8 we find $\boldsymbol{f}_0 \in N$ in $\mathsf{D}\left(s,\ x_0\boldsymbol{\epsilon}_j\right)$ for some $x_0 \in \mathbb{N}$ and of weight greater than d_0, such that $\mathsf{A}\left(0,\ (p-1)\mathbf{1},\ \boldsymbol{f}_0,\ 1\right)$ is not empty. Moreover, every $\boldsymbol{g} \in \mathcal{G}\ell_n^1$ is trivially in $\mathsf{S}\left(0,\ d\right)$ for any $d \in \mathbb{N}$, so we may safely assume that $\boldsymbol{f}_0$ is in $\mathsf{S}\left(0,\ d_0\right)$.

By Corollary 6.12 applied to $l = 0$, $\boldsymbol{f}_0$ and $v = v_0$, there exists $\boldsymbol{f}_1 \in N$ that is in $\mathsf{D}\left(s,\ x_1\boldsymbol{\epsilon}_j\right)$ for some $x_1 \in \mathbb{N}$ and in $\mathsf{S}\left(1,\ d_1\right)$.

Now we apply Proposition 6.14 to $\boldsymbol{f}_1$, $l_1 = 1$, $l_2 = s$, $i \in \mathbb{N}$ and we obtain $\boldsymbol{f}_s$ in $\mathsf{D}\left(s,\ x_s\boldsymbol{\epsilon}_j\right)$ for some $x_s \in \mathbb{N}$ and in $\mathsf{S}\left(s,\ d_s\right)$, that is $(\boldsymbol{\alpha}, k) \in \mathrm{Supp}_1\boldsymbol{f}_s$ only if $k = i$, $\boldsymbol{\alpha} = p^s\Psi_s\left(\boldsymbol{\alpha}\right)$ and $\Psi_s\left(\boldsymbol{\alpha}\right) = x_s\boldsymbol{\epsilon}_j$. This means that $\boldsymbol{f}_s \equiv \boldsymbol{t} + t_j^{p^s x_s}\boldsymbol{E}_i$ modulo $\mathcal{M}^{\omega(\boldsymbol{f})+d_s+1}$. So we may apply Lemma 6.7 and find that N contains $\mathcal{K}\left(\mathfrak{m}^{x_s+2m+1} \cap (t_j^{x_s})\right)$. Since j was arbitrarily chosen and x_s does not depend on j, using Proposition 5.3, we obtain that N contains $\mathcal{K}\left(\mathfrak{m}^{x_s+2m+1} \cap \left((t_1^{x_s}) + \ldots + (t_n^{x_s})\right)\right)$. Consider $I = (t_1^{x_s}) + \ldots + (t_n^{x_s})$. Let $\boldsymbol{\alpha}$ be of weight greater than or equal to nx_s. Then $\boldsymbol{\alpha} \geq x_s\boldsymbol{\epsilon}_j$ for some $j \in \{1, \ldots, n\}$, that is $\boldsymbol{t}^{\boldsymbol{\alpha}} \in I$. Thus I contains $\mathfrak{m}^{x_s n}$ and in particular $I \cap \mathfrak{m}^{x_s+2m+1}$ is open. By Proposition 5.3, we have that $\mathcal{K}\left(\mathfrak{m}^{x_s+2m+1} \cap I\right)$ is open and so it is N that contains it. □

6.4 Quantitative version of Theorem 0.2

So we proved that the generalized Nottingham group is hereditarily just infinite. Now we may wonder "how much" it is hereditarily just infinite. In this section we are going to review the proof, in order to prove not only hereditarily just infiniteness of $\mathcal{G}\ell_n^1$, but also how large a normal subgroup should be. In order to get a better result, we slightly change the just shown proof. Indeed this developed by steps taking every time an element $\boldsymbol{f}_i \in N$ in $\mathsf{D}\left(s,\ \boldsymbol{\chi}_{i-1} + \boldsymbol{\beta}_i\right)$ with $\boldsymbol{\chi}_{i-1}$ depending on $\boldsymbol{f}_{i-1}$ and $\boldsymbol{\beta}_i = x_i \boldsymbol{\epsilon}_j$ for some $x_i \in \mathbb{N}$. However we might exploit the more freedom our tools give us to choose $\boldsymbol{\beta}_i$ other than n-tuples of the form $x_i\boldsymbol{\epsilon}_j$.

Before, however we prove a lemma we are going to use later.

Lemma 6.16. *Let s and m be positive integers and let $(d_i)_{i=0}^s$ and $(v_i)_{i=0}^{s-1}$ be the integer sequences defined in* (6.3) *for any $d_s \in \mathbb{N}$. Then $v_l \leq v_{l+1} + \lceil \log_p(n) \rceil + 2$ for every $0 \leq l < s-1$*

Proof. Since $v_{l+1} \geq s$ and $p^{v_{l+1}} > m$ by construction, we trivially have that also $v_{l+1} + \lceil \log_p(n) \rceil + 2$ satisfies the same conditions. Thus we only need to verify that $p^l(p-1)\left(p^{v_{l+1}+\lceil \log_p(n) \rceil + 2} - 1\right)$, that is denoted by r, is greater than or equal to d_{l+1}. Let us write just v instead of v_{l+1}. So

$$
\begin{aligned}
r = p^l(p-1)\left(p^{v+\lceil \log_p(n)\rceil+2} - 1\right) \geq p^l(p-1)\left(np^2p^v - 1\right) \geq& \\
\geq p^l(p-1)p(p^v-1) + p^l(p-1)(np^2p^v - 1 - pp^v + p)&
\end{aligned}
$$

where by construction $p^l(p-1)p(p^v-1) \geq d_{l+2}$ and therefore

$$
r \geq d_{l+2} + p^l(p-1)(np^2p^v - 1 - pp^v + p).
$$

Now we have

$$
np^2p^v - 1 - pp^v + p \geq (np-1)pp^v + p - 1 \geq (np-1)p(p^v-1) \geq np(p^v-1)
$$

implying that $r \geq d_{l+2} + n(p^{l+1}-1)(p-1)(p^v-1) = d_{l+1}$. Then the claim follows from the definition of v_l. □

In our proof of Theorem 0.2 we started from a non-trivial element $\boldsymbol{f}$ of the normal subgroup N of an open subgroup containing $\mathcal{G}\ell_n^m$. We noticed that $\boldsymbol{f}$ is in $\mathsf{D}\left(0,\ s-2\right)$ for s such that $p^{s-2} > \omega\left(\boldsymbol{f}\right) + 1$. In the first step we find $\boldsymbol{f}_0$ applying Lemma 6.8. Such an element is in $\mathsf{D}\left(s,\ \boldsymbol{\beta}_0\right)$ for any $\boldsymbol{\beta}_0 \in {\mathbb{N}_0}^n$ such that $p^s\lfloor|\boldsymbol{\beta}_0|/2\rfloor > m$ and must be of weight at least d_0. Note that $p^s\lfloor|p^{v_0-p^s}(p-1)n|/2\rfloor > m$ and by definition p^{v_0} is at least d_0, so we may assume $p^s\boldsymbol{\beta}_0 = p^{v_0}\tilde{\boldsymbol{\beta}}_0$ for an arbitrary $\tilde{\boldsymbol{\beta}}_0$ of weight $(p-1)n$. With an abuse of notation, we write $\boldsymbol{\beta}_0$ meaning $\tilde{\boldsymbol{\beta}}_0$, so that $\boldsymbol{f}_0$ is in $\mathsf{D}\left(s,\ p^{v_0-s}\boldsymbol{\beta}_0\right)$. Then $\boldsymbol{f}_1$ is obtained by Corollary 6.12 and so it is in $\mathsf{D}\left(s,\ p^{v_0-s}\left(\boldsymbol{\beta}_0 + \boldsymbol{\eta}_0\right)\right)$ where $|\boldsymbol{\eta}_0| = n(p-1)$. Proceeding in the review of the proof, we have $\boldsymbol{f}_s$ that is the result of Proposition 6.14 and therefore it is in $\mathsf{S}\left(s,\ d_s\right)$ and in $\mathsf{D}\left(s,\ \sum_{l=0}^{s-1}(p^{v_l-s}\boldsymbol{\beta}_l + p^{v_l+l-s}\boldsymbol{\eta}_l)\right)$, where each $\boldsymbol{\eta}_l \in {\mathbb{N}_0}^n$ is only required to have weight $n(p-1)$ while $\boldsymbol{\beta}_l \in {\mathbb{N}_0}^n$ has weight $n(p-1) - \mathit{\Psi}_l\left(\boldsymbol{\gamma}\right) - p\mathit{\Psi}_{l+1}\left(\boldsymbol{\gamma}\right)$ for every $1 \leq l < s$, where $(\boldsymbol{\gamma}, k)$ is a fixed element of $\mathrm{Supp}_1\boldsymbol{f}_1$. In particular, for every $l \in \{0, \dots, s-1\}$, both $\boldsymbol{\beta}_l$ and $\boldsymbol{\eta}_l$ have weight at most $(p-1)n$.

Since $\boldsymbol{f}_s$ is also in $\mathsf{S}\left(s,\ 1\right)$, its restricted 1-support is exactly $\{(\sum_{l=0}^{s-1}(p^{v_l}\boldsymbol{\beta}_l + p^{v_l+l}\boldsymbol{\eta}_l), i)\}$ for an arbitrary $i \in \{1, \dots, n\}$. Let $\boldsymbol{\delta}$ denote $\sum_{l=0}^{s-1}(p^{v_l}\boldsymbol{\beta}_l + p^{v_l+l}\boldsymbol{\eta}_l)$. By Lemma 6.7, we have that N contains $\mathcal{K}\left(\left(\boldsymbol{t}^{\boldsymbol{\delta}}\right) \cap \mathfrak{m}^{|\boldsymbol{\delta}|+2m+2}\right)$. Let w denote $\sum_{l=0}^{s-1}(p^{v_l} + p^{v_l+l})$ and consider any $\boldsymbol{\zeta} \in {\mathbb{N}_0}^n$ of weight npw. We may write $\boldsymbol{\zeta}$ as $\sum_{l=0}^{s-1}\left(\boldsymbol{\zeta}_l + \boldsymbol{\zeta}_l'\right)$ where $|\boldsymbol{\zeta}_l| = npp^{v_l}$ and $|\boldsymbol{\zeta}_l'| = npp^{v_l+l}$ for every $l \in \{0, \dots, s-1\}$. Then for every $l \in \{0, \dots, s-1\}$ there exists at least one choice for each $\boldsymbol{\beta}_l$ and each $\boldsymbol{\eta}_l$ such that $p^{v_l}\boldsymbol{\beta}_l \leq \boldsymbol{\zeta}_l$ and $p^{v_l+l}\boldsymbol{\eta}_l \leq \boldsymbol{\zeta}_l'$ for every $l \in \{0, \dots, s-1\}$ (see Lemma B.14). Moreover $|\boldsymbol{\zeta}| = npw = n(p-1)w + nw \geq |\boldsymbol{\delta}| + 2m + 2$ since each p^{v_l} is greater than m. So we have that $\boldsymbol{t} + \boldsymbol{t}^{\boldsymbol{\zeta}}\boldsymbol{E}_i$ is in N for every $\boldsymbol{\zeta}$ of weight npw and every $i \in \{1, \dots, n\}$. But these elements generate $\mathcal{G}\ell_n^{npw-1}$, that therefore is contained in N.

It only remains to give an upper bound for w in terms of n, p, m and $\omega(\boldsymbol{f})$. By Lemma 6.16 we have $v_l \leq v_{s-1} + (s-1-l)(\lceil \log_p(n) \rceil + 2)$, hence we can write

$$\begin{aligned} w &\leq \sum_{l=0}^{s-1} \left(p^{v_{s-1}+(s-1-l)(\lceil \log_p(n)\rceil+2)} + p^{v_{s-1}+(s-1-l)(\lceil \log_p(n)\rceil+2)+l} \right) \\ &\leq p^{v_{s-1}} \sum_{l=0}^{s-1} \left(\left(p^{\lceil \log_p(n)\rceil+2} \right)^l + p^{(s-1-l)(\lceil \log_p(n)\rceil+2)+l} \right) \end{aligned}$$

where $(s-1-l)(\lceil \log_p(n) \rceil + 2) + l$ equals $(s-1) + (\lceil \log_p(n) \rceil + 1)(s-1-l)$ and therefore $\sum_{l=0}^{s-1} p^{(s-1-l)(\lceil \log_p(n)\rceil+2)+l} = p^{s-1} \sum_{l=0}^{s-1} (p^{\lceil \log_p(n)\rceil+1})^l$. Thus

$$\begin{aligned} w &\leq p^{v_{s-1}} \left(\frac{\left(p^{\lceil \log_p(n)\rceil+2}\right)^s - 1}{p^{\lceil \log_p(n)\rceil+2} - 1} + p^{s-1} \frac{\left(p^{\lceil \log_p(n)\rceil+1}\right)^s - 1}{p^{\lceil \log_p(n)\rceil+1} - 1} \right) \\ &\leq p^{v_{s-1}} \left(\frac{(p^s)^{\lceil \log_p(n)\rceil+2} - 1}{p^{\lceil \log_p(n)\rceil+2} - 1} + \frac{(p^s)^{\lceil \log_p(n)\rceil+2} - p^s}{p^{\lceil \log_p(n)\rceil+2} - p} \right). \end{aligned}$$

Since $n \leq p^{\lceil \log_p(n) \rceil} < pn$ and s can be chosen so that $p^2(\omega(\boldsymbol{f}) + 1) < p^s \leq p^3(\omega(\boldsymbol{f}) + 1)$, we obtain

$$w \leq p^{v_{s-1}} \left(\frac{\left(p^3\left(\omega(\boldsymbol{f})+1\right)\right)^{\lceil \log_p(n)\rceil+2} - 1}{p^2 n - 1} + \frac{\left(p^3\left(\omega(\boldsymbol{f})+1\right)\right)^{\lceil \log_p(n)\rceil+2} - p^3(\omega(\boldsymbol{f})+1)}{p^2 n - p} \right).$$

Finally observe that if $d_s = 1$ — and we can always assume so — then $v_{s-1} = \max\{\lfloor \log_p(m) \rfloor + 1, s\}$, thus $p^{v_{s-1}}$ is always less than or equal to $\max\{pm, p^3(\omega(\boldsymbol{f}) + 1)\}$.

Therefore we have proved

Theorem 6.17. *Let O be an open subgroup of $\mathcal{G}\ell_n^1$ containing $\mathcal{G}\ell_n^m$ for some $m \in \mathbb{N}$ and let N be a closed normal subgroup of O. Suppose $N \not\leq \mathcal{G}\ell_n^r$ for some $r \in \mathbb{N}$ (i. e. there exists $\boldsymbol{f} \in N$ of depth $r-1$). Then N contains $\mathcal{G}\ell_n^{u(r,m)-1}$, where*

$$u(r,m) = \max\{pm, p^3 r\} np \left(\frac{(p^3 r)^{\lceil \log_p(n)\rceil+2} - 1}{p^2 n - 1} + \frac{(p^3 r)^{\lceil \log_p(n)\rceil+2} - p^3 r}{p^2 n - p} \right).$$

Remark 6.18. In particular the function $u(r,m)$ is asymptotic to $(p^3 r)^{\lceil \log_p(n)\rceil+3} \frac{2p^n - p - 1}{(p^2 n - 1)(p^2 n - p)}$ as r tends to infinity.

Chapter 7

Abstract randomly generated subgroups

7.1 Probabilistic identities

Let G be a profinite group. Since it is compact there exists a unique normalized Haar measure μ_G for it, obtained by imposing

$$\mu_G(H) = |G : H|^{-1}$$

for every open (i. e. finite index) subgroup of G. This is enough to determine it, since cosets of open subgroups generate the topology and hence the Borel σ-algebra. In this way we turn G into a probabilistic space.

In late '90s this point of view in the study of profinite groups knew intensive research. Results in this area usually aim to determine what can be said about a group in which we know some probabilistic identity is satisfied. A group is said to satisfy an identity $w(x_1, \dots, x_m) = 1$ — where $w(x_1, \dots, x_m)$ is a word in m indeterminates — if $w(g_1, \dots, g_m) = 1$ for every $g_1, \dots, g_m \in G$, while it is said to satisfy a probabilistic identity $w(x_1, \dots, x_m) = 1$ if the set of n-tuples in G^n that satisfy it have positive measure.

In this perspective, Shalev [35] stated some very strong and still open conjectures, among which there is the following (Conjecture 2): let G be a finitely generated pro-p group satisfying some probabilistic identity, then it satisfy a related identity.

A consequence [35, Problem 7] of this last conjecture is that any finitely generated pro-p group which contain an abstract free subgroup of rank $d \in \mathbb{N}$ should not satisfy any probabilistic identities. In other words: any d randomly chosen element of G should generate with probability 1 an abstract free subgroup.

Since the Nottingham group contains an abstract free subgroup of rank d for every $d \in \mathbb{N}$, it was a good candidate to test such conjecture.

So, in 2005, Szegedy [39] proved that the conjecture holds for the classic Nottingham group. In this chapter we extend his proof to the generalized Nottingham group, that is, we prove the following theorem.

Theorem 7.1. *Every k-tuple of randomly chosen elements in $\mathcal{G}\ell_n^1(\mathbb{F}_p)$ generate with probability one an abstract free group of rank k.*

7.2 Proof of the theorem

This is one of the few cases in which an interesting result about the generalized Nottingham group can be achieved by an easy extension of the proof for the analogous result in the classical case. So most of the following considerations, formulae and results are somewhat natural extensions and the only real necessary improvement to make all these work is the use of Proposition 1.12.

So, we proceed along Szegedy's work. In particular, the entire proof relies on [39, Lemma 9], whose statement is quoted below.

Lemma 7.2. *Let G be a pro-p group with open normal subgroups G_i, M_i — $i \in \mathbb{N}$ — such that the following statements hold.*

(1) The sequence G_i is a filtration of G.

(2) $G_i > M_i$ for all $i \in \mathbb{N}$.

(3) The factors G_i/M_i are elementary abelian p-groups for all $i \in \mathbb{N}$.

(4) The images of the group elements are linearly independent under the natural map

$$\begin{aligned}\sigma : G \mapsto & \mathrm{End}_{\mathbb{F}_p}\left(\bigoplus_{i \geq k} G_i/M_i\right)\\ g \mapsto & \left(\sigma_g : (v_k, v_{k+1}, \dots) \mapsto (v_k^g, v_{k+1}^g, \dots)\right)\end{aligned}$$

for all natural numbers k.

Then two random elements of G generate a free group with probability 1.

Szegedy himself observed in his paper that this lemma might be extended to show that in the same hypothesis, any d random elements of G generate an abstract free group with probability 1. For the sake of completeness, this extended version of Lemma 7.2 is made available in Appendix C (Lemma C.3).

However, before applying this lemma, we need some variations to formulae given in Chapter 1. By equation (1.7) we obtain that for every $\boldsymbol{f} = \boldsymbol{t} + \boldsymbol{f}'$ and $\boldsymbol{g} = \boldsymbol{t} + \boldsymbol{g}'$ in $\mathcal{G\ell}_n(\mathbb{F}_q)$

$$\boldsymbol{f} \circ \boldsymbol{g} \equiv \boldsymbol{t} + \boldsymbol{f}' + \boldsymbol{g}' + \sum_{i=1}^{n} g_i \partial_{\boldsymbol{\epsilon}_i} \boldsymbol{f} \mod \mathcal{M}_n^{2\,\omega(\boldsymbol{g})+\omega(\boldsymbol{f})+1}(R)$$

where $\boldsymbol{g}' = (g_i)_{i=1}^n$. Hence, since $\partial_{\boldsymbol{\epsilon}_i} = \partial_i$ for every $i \in \{1, \dots, n\}$,

$$\boldsymbol{f} \circ \boldsymbol{g} \equiv \boldsymbol{t} + \boldsymbol{f}' + \sum_{i=1}^{n} g_i \partial_i(\boldsymbol{f}) \equiv \boldsymbol{f} + \mathrm{Jac}(\boldsymbol{f}) \cdot \boldsymbol{g}' \tag{7.1}$$

modulo $\mathcal{M}_n^{2\,\omega(\boldsymbol{g})+\omega(\boldsymbol{f})+1}(R)$. We use this last formula to prove

Lemma 7.3. *Let $\boldsymbol{f} = \boldsymbol{t} + \boldsymbol{f}'$ and $\boldsymbol{g} = \boldsymbol{t} + \boldsymbol{g}'$ be in $\mathcal{G\ell}_n(\mathbb{F}_q)$. Then*

$$\boldsymbol{f}^{\boldsymbol{g}} = \boldsymbol{g}^{-1} \circ \boldsymbol{f} \circ \boldsymbol{g} \equiv \boldsymbol{t} + \mathrm{Jac}(\boldsymbol{g})^{-1} \cdot (\boldsymbol{f}' \circ \boldsymbol{g})$$

modulo $\mathcal{M}_n^{2\,\omega(\boldsymbol{f})+1}(R)$.

Proof. Let $\boldsymbol{h}$ denote $\boldsymbol{f}^{\boldsymbol{g}}$ and let $\boldsymbol{h}'$ be $\boldsymbol{h}-\boldsymbol{t}$. Since $\boldsymbol{g}\circ\boldsymbol{h}=\boldsymbol{f}\circ\boldsymbol{g}$, by formula (7.1), we have

$$\boldsymbol{g}+\mathrm{Jac}(\boldsymbol{g})\cdot\boldsymbol{h}'\equiv\boldsymbol{f}\circ\boldsymbol{g}\mod \mathcal{M}_n^{2\,\omega(\boldsymbol{h})+\omega(\boldsymbol{g})+1}(R)$$

whence

$$\boldsymbol{h}\equiv\boldsymbol{t}+\mathrm{Jac}(\boldsymbol{g})^{-1}\cdot(\boldsymbol{f}\circ\boldsymbol{g}-\boldsymbol{g})\mod \mathcal{M}_n^{2\,\omega(\boldsymbol{h})+\omega(\boldsymbol{g})+1}(R)$$

where $\boldsymbol{f}\circ\boldsymbol{g}-\boldsymbol{g}=\boldsymbol{f}'\circ\boldsymbol{g}$ since $\boldsymbol{f}\circ\boldsymbol{g}=\boldsymbol{t}\circ\boldsymbol{g}+\boldsymbol{f}'\circ\boldsymbol{g}$. So we can observe that $\omega(\boldsymbol{h})=\omega(\boldsymbol{f})$ and the claim follows immediately. □

Remark 7.4. If $\boldsymbol{g}=\boldsymbol{t}+\boldsymbol{g}'$ is in $\mathcal{G}\ell_n^1(\mathbb{F}_q)$, that is $\boldsymbol{g}'$ has order at least 2, then $\mathrm{Jac}(\boldsymbol{g})=\mathrm{id}+M$ where id is the identity $n\times n$ matrix and M is an $n\times n$ matrix whose entries are in $\mathfrak{m}$. Thus also its inverse have this form.

Remark 7.5. We have not used the hypothesis $R=\mathbb{F}_q$ in any part of the proof that therefore holds for arbitrary rings.

We will apply Lemma 7.2 with $G_i=\mathcal{G}\ell_n^i(\mathbb{F}_q)$ and $M_i=\mathcal{G}\ell_n^{2i}(\mathbb{F}_q)$, therefore it suffices to show that for every finite subset $\{\boldsymbol{g}_j\mid 1\le j\le r\}$ of $\mathcal{G}\ell_n^1(\mathbb{F}_q)$, the images of each $\boldsymbol{g}_j$ through the application described in the lemma are linearly independent.

Suppose there exists $\lambda_j\in\mathbb{F}_p$ for every $1\le j\le r$ such that $u:=\sum_{j=1}^r\lambda_j\sigma_{\boldsymbol{g}_j}$ is the trivial application. Then for every $i\in\mathbb{N}$ and every $\boldsymbol{h}\in\mathcal{G}\ell_n^i(\mathbb{F}_q)$, we have $(\boldsymbol{h}\mathcal{G}\ell_n^{2i}(\mathbb{F}_q))^u=\mathcal{G}\ell_n^{2i}(\mathbb{F}_q)$, that is, by Lemma 7.3 and identifying $\mathcal{G}\ell_n^i(\mathbb{F}_q)/\mathcal{G}\ell_n^{2i}(\mathbb{F}_q)$ with $\mathcal{M}_n^{i+1}(R)/\mathcal{M}_n^{2i+1}(R)$ as in Corollary 1.20,

$$\sum_{j=1}^r\mu_j\cdot(\boldsymbol{h}-\boldsymbol{t})\circ\boldsymbol{g}_j\equiv 0\mod \mathcal{M}_n^{2i+1}(R)$$

where each μ_j denotes the matrix $\lambda_j\mathrm{Jac}\left(\boldsymbol{g}_j\right)^{-1}$.

For every $j\in\{1,\dots,r\}$, let ϕ_j be the automorphism of $\mathbb{F}_q[\![\boldsymbol{t}]\!]$ that by Proposition 1.6 is associated to $\boldsymbol{g}_j$. Let A_0 be the open set $t_1+\mathfrak{m}^2$. Recursively, for all $k\in\{1,\dots,n\}$, we fix an element f_k of A_k, where A_k is the open subset of

$$A_{k-1}\setminus\left\{\phi_j^{-1}\phi_i(f_l)\mid i,j\in\{1,\dots,r\},\ l\in\{1,\dots,k-1\}\right\}$$

resulting from Proposition 1.12 applied to $\phi_1,\dots,\phi_r$. Thus we obtain a set

$$\{f_k=t_1+r_k\in\mathbb{F}_q[\![\boldsymbol{t}]\!]\mid r_k\in\mathfrak{m}^2,\ 1\le k\le n\}\subseteq\mathbb{F}_q[\![\boldsymbol{t}]\!]$$

of formal power series such that $f_k\circ\boldsymbol{g}_i=\phi_i(f_k)$ equals $f_l\circ\boldsymbol{g}_j=\phi_j(f_l)$ if and only if $i=j$ and $k=l$.

Fix $s,m\ge 0$ and let a be a positive integer such that $p^a>s$ and $p^a+s>m$. Let i equal p^a+s (so $i\ge m$) and choose $\boldsymbol{h}$ to be $(t_k+{f_k}^i)_{k=1}^n\in\mathcal{G}\ell_n^i(\mathbb{F}_q)$. Then, letting $\boldsymbol{f}$ denote $(f_k)_{k=1}^n$, we have $0\equiv\sum_{j=1}^r\mu_j\cdot(\boldsymbol{f}^i\circ\boldsymbol{g}_j)$ modulo $\mathcal{M}_n^{2i+1}(R)$ and, since $2i+1\ge 2p^a$, the equivalence holds also modulo $\mathcal{M}_n^{2p^a}(R)$. When we expand $\boldsymbol{f}^i$, we obtain

$$\boldsymbol{f}^i=\left({f_k}^{p^a}{f_k}^s\right)_{k=1}^n=\left(\left((t_1)^{p^a}+(r_k)^{p^a}\right){f_k}^s\right)_{k=1}^n\equiv\left((t_1)^{p^a}{f_k}^s\right)_{k=1}^n\mod \mathcal{M}_n^{2p^a}(R)$$

so that

$$0\equiv\sum_{j=1}^r\mu_j\cdot\left(({t_1}^{p^a}{f_k}^s)_{k=1}^n\circ\boldsymbol{g}_j\right)\equiv{t_1}^{p^a}\sum_{j=1}^r\mu_j\cdot(\boldsymbol{f}\circ\boldsymbol{g}_j)^s\mod \mathcal{M}_n^{2p^a}(R)$$

since ${(t_1{}^{p^a} f_k{}^s)} \circ \boldsymbol{g}_j = (t_1 \circ \boldsymbol{g}_j)^{p^a} (f_k \circ \boldsymbol{g}_j)^s$ and $(t_1 \circ \boldsymbol{g}_j)^{p^a} \equiv t_1^{p^a}$ modulo $\mathcal{M}_n^{2p^a}(R)$ for all $1 \leq j \leq r$ and $1 \leq k \leq n$. It follows that $0 \equiv \sum_{j=1}^{r} \mu_j \cdot (\boldsymbol{f} \circ \boldsymbol{g}_j)^s$ modulo $\mathcal{M}_n^{p^a}(R)$. As s is completely arbitrary while a is arbitrarily large we have

$$0 = \sum_{j=1}^{r} \mu_j \cdot (\boldsymbol{f} \circ \boldsymbol{g}_j)^s$$

for every $s \in \mathbb{N}_0$, in particular for $0 \leq s \leq r \times n$. We can write this condition as a product of matrices $0 = M \cdot V$, where M is a block matrix defined by

$$M = \begin{pmatrix} \mu_1 & \mu_2 & \cdots & \mu_r \end{pmatrix}$$

whereas

$$V = \begin{pmatrix} (\boldsymbol{f} \circ \boldsymbol{g}_1)^0 & (\boldsymbol{f} \circ \boldsymbol{g}_1)^1 & \cdots & (\boldsymbol{f} \circ \boldsymbol{g}_1)^{rn} \\ (\boldsymbol{f} \circ \boldsymbol{g}_2)^0 & (\boldsymbol{f} \circ \boldsymbol{g}_2)^1 & \cdots & (\boldsymbol{f} \circ \boldsymbol{g}_2)^{rn} \\ \vdots & \vdots & & \vdots \\ (\boldsymbol{f} \circ \boldsymbol{g}_r)^0 & (\boldsymbol{f} \circ \boldsymbol{g}_r)^1 & \cdots & (\boldsymbol{f} \circ \boldsymbol{g}_r)^{rn} \end{pmatrix} = \begin{pmatrix} 1 & (f_1 \circ \boldsymbol{g}_1)^1 & \cdots & (f_1 \circ \boldsymbol{g}_1)^{nr} \\ 1 & (f_2 \circ \boldsymbol{g}_1)^1 & \cdots & (f_2 \circ \boldsymbol{g}_1)^{nr} \\ \vdots & \vdots & & \vdots \\ 1 & (f_1 \circ \boldsymbol{g}_2)^1 & \cdots & (f_1 \circ \boldsymbol{g}_2)^{nr} \\ \vdots & \vdots & & \vdots \\ 1 & (f_n \circ \boldsymbol{g}_r)^1 & \cdots & (f_n \circ \boldsymbol{g}_r)^{nr} \end{pmatrix}$$

is an $nr \times nr$ Vandermonde matrix. Since all $f_k \circ \boldsymbol{g}_j$ are pair-wise distinct, the matrix V is invertible (in the quotient field of $\mathbb{F}_q[\![\boldsymbol{t}]\!]$), thus M must be 0. As all matrices $\operatorname{Jac}(\boldsymbol{g}_j)^{-1}$ are obviously non-trivial, this implies that each coefficient λ_j is 0.

Chapter 8

Conclusions

So we have given a complete — to some extent — introduction of the generalized Nottingham group and some classes of related groups. Still, much has to be done.

Remark 8.1. Many of the claims stated in this chapter are speculations that should be carefully verified.

Concerning just infiniteness

While we know that the generalized Nottingham group over a finite field of odd characteristic is hereditarily just infinite, the question is still open for characteristic 2 fields and the other Cartan type groups. We have already noticed that also for $n = 1$, the proof of hereditarily just infiniteness for odd characteristic field is completely different, thus also for $n \geq 2$ we expect something similar to happen.

In general, for Cartan type groups things are still very unclear. However for the special group there are strong evidences for it to be h. j. i., and we are not so far from a proof. Indeed, with some minor caveat, stages 3 and 4 of Section 6.2 holds also for the special group, whereas Lemma 6.7 should have a sort of corresponding result. Thus, it only remains to prove something like the second stage and we do not expect it to be very hard to solve.

It would be desirable there existed some general proof of just infiniteness for Cartan type groups. We want to remark that this could not rely entirely on the associated algebra. Consider for example the subgroup $\mathcal{K}\left((\boldsymbol{t}^{p\boldsymbol{\alpha}})\right) \leq \mathcal{G}\ell_n^1(\mathbb{F}_q)$ associated to the ideal of $\mathbb{F}_q[\![\boldsymbol{t}]\!]$ generated by $\boldsymbol{t}^{p\boldsymbol{\alpha}}$ for some $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n \setminus \{\boldsymbol{0}\}$. Then the associated subalgebra of $L(\mathcal{G}\ell_n^1(\mathbb{F}_q))$, that is contained in the subalgebra associated to any Cartan type subgroup, is in fact an ideal, although the subgroup is not normal. Thus it is not possible recover just infiniteness of the generalized Nottingham group — or other Cartan type groups — simply from its associated algebra, differently to what happens for the classic Nottingham group.

Differences between classic and generalized Nottingham group

The result proved in Chapter 7 is somewhat a simple extension of the corresponding result for the classic Nottingham group, and also the technics we used for the proof are not so different with respect to the case $n = 1$. However this is quite an exception, rather than a rule. There is plenty of results about the Nottingham group that cannot be easily extended. Some examples are the fact that it is finitely presented [16], the explicit expression for its abstract commensurator group [15] and — of course — its just infiniteness. The point is that many of these proofs rely

— either explicitly or implicitly — on the fact that the classic Nottingham group over a finite field has finite width, whereas from Corollary 1.20 and Corollary 2.14 we know that this is not the case when $n \geq 2$. Thus the generalized group often require much more effort.

When $p \geq 5$, we know [22, 15] that both the automorphism group and the commensurator group of $\mathrm{Aut}\mathbb{F}_p[\![t]\!]$ coincide with $\mathrm{Aut}\mathbb{F}_p[\![t]\!]$ itself, thus the Nottingham group, that is a normal subgroup of it, is somewhat more than characteristic. However, it was already known a priori that it is characteristic — over any finite field $\mathbb{F}_q$ of order a p-power q — since it is the unique p-Sylow subgroup of $\mathrm{Aut}\mathbb{F}_p[\![t]\!] \cong \mathbb{F}_p^\times \ltimes \mathcal{G}\ell_1(\mathbb{F}_p)$. As we have already pointed out, so far we do not have any analogous result to the above cited ones for $n \geq 2$, and the generalized Nottingham group it is not even a p-Sylow subgroup. However it is still a characteristic subgroup — for odd prime p — of $\mathrm{Aut}_{\mathfrak{m}}\mathbb{F}_q[\![\boldsymbol{t}]\!]$, that since $\mathbb{F}_q$ is a field coincides with $\mathrm{Aut}\mathbb{F}_q[\![\boldsymbol{t}]\!]$ (see Remark 1.10). In fact, the p-Sylow subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$ are the maximal unipotent subgroups [42] and their intersection is trivial, thus, since $\mathrm{Aut}_{\mathfrak{m}}\mathbb{F}_q[\![\boldsymbol{t}]\!] \cong \mathrm{GL}_n(\mathbb{F}_q) \ltimes \mathcal{G}\ell_n^1(\mathbb{F}_q)$ by Proposition 1.14, the intersection of all p-Sylow subgroups of it is exactly $\mathcal{G}\ell_n^1(\mathbb{F}_q)$. It follows that also $\mathcal{G}\ell_n^i(\mathbb{F}_q)$ is characteristic for every $i \in \mathbb{N}$, since it is the i-th term of the lower central series (Corollary 2.14).

About pseudo-algebraic groups

Chapter 4 looks like a little inconclusive. The reason is a lack of both time to properly develop the topic and a clear view on the subject. The idea behind the introduction of pseudo-algebraic groups was to give another tool to study Cartan type groups. In the chapter we pointed out the case of the special group that is the intersection of the pseudo-algebraic group associated to SL_n with the Nottingham group. In some sense, we may say that the special Cartan type group is the "first congruence subgroup" of $\mathcal{S}\ell_n(R)$ as well as so it is the Nottingham group for $\mathcal{G}\ell_n(R)$. Something similar may be done also for other Cartan type groups. Indeed an automorphism that fixes a differential form ω must satisfy some differential equations that in turn can be expressed as polynomial conditions on the Jacobian and therefore a Cartan type sugroup may be seen again as the "first congruence subgroup" of a pseudo-algebraic group. Moreover, let $\boldsymbol{t} + \tau\boldsymbol{f}$ be in the Lie ring of $\mathcal{G}\ell_n(R)$. Then it acts on ω like $\mathrm{id} + \tau D_{\boldsymbol{f}}$ where $D_{\boldsymbol{f}}$ is the associated derivations. So

$$(\mathrm{id} + \tau D_{\boldsymbol{f}})\omega = \omega + \tau D_{\boldsymbol{f}}\omega$$

equals ω if and only if $D_{\boldsymbol{f}}\omega = 0$, that is to say derivations in the Lie ring of the pseudo-algebraic group are those that annihilate the differential form. So the Lie ring of the pseudo-algebraic group associated to a Cartan type subgroup is the intersection of the Cartan type algebra and $\mathrm{Der}_R^0(R[\![\boldsymbol{t}]\!])$ (for the contact subgroup things work slightly differently).

About the associated Lie ring. Consider an element $\boldsymbol{t}+\tau\boldsymbol{f}$ in the Lie ring of a pseudo-algebraic group $\mathcal{G}(R)$ over a ring K. Then its Jacobian matrix is of the form

$$\mathrm{id} + \tau\mathrm{Jac}(\boldsymbol{f})$$

where id denotes the identity matrix. Let P be a polinomyal in $K[X_{1,1}, \ldots, X_{n,n}]$ defining the associated algebraic group and write $(f_i)_{i=1}^n$ for $\boldsymbol{f}$. Since $\tau^2 = 0$, when we evaluate P on $\mathrm{id} + \tau\mathrm{Jac}(\boldsymbol{f})$, we obtain something of the form

$$c + \tau \sum_{i,j=1}^{n} a_{i,j}\partial_j f_i$$

that should be zero. Thus both c and $\sum_{i,j=1}^{n} a_{i,j}\partial_j f_i$ are null. It follows that, for every $r \in R$, also $\boldsymbol{t} + \tau r\boldsymbol{f}$ is in $\mathrm{Lie}(\mathcal{G})(R)$ that, therefore, has a structure of Lie R-algebra.

We conclude these considerations about the Lie ring with a conjecture.

Conjecture 1. The intersection of the Lie ring associated to a pseudo-algebraic group $\mathcal{G}(R)$ with $\mathrm{Der}^1_R(R[\![\boldsymbol{t}]\!])$ coincides with the Lie ring in the sense of Chapter 2 of $\mathcal{G}(R) \cap \mathcal{G}\ell^1_n(R)$.

Note that index-subgroups behave somehow similarly to pseudo-algebraic subgroup. The intersection of these two families of groups is not trivial, as it can be seen from examples shown in Chapter 4 and Section 5.2. Actually, fixed *any* ring K, then it is possible to define the concept of admissible index-set (in the definition, instead of requiring $\binom{\boldsymbol{\beta}}{h\boldsymbol{\epsilon}_i} \not\equiv_p 0$, we ask the natural image of $\binom{\boldsymbol{\beta}}{h\boldsymbol{\epsilon}_i} \in \mathbb{Z}$ into K not to be 0) and Lemma 5.5 still works. Moreover, any index-set that is admissible for K is also admissible for any K-algebra R. Thus we can construct a map — that eventually is a functor — from K-algebras to groups, associated to the admissible index-set. We can also define — in the same way we did for pseudo-algebraic subgroups — an associated Lie algebra and it should be easy to verify that indeed such a Lie algebra is isomorphic to the Lie algebra described in Chapter 2 (when we restrict to subgroups of the Nottingham group). So, the feeling is that both pseudo-algebraic groups and index-subgroups are part of a larger family of subgroups of $\mathcal{G}\ell_n(R)$ that indeed are images of functors from K-algebras to groups.

We may also use pseudo-algebraic groups to introduce another kind of Cartan type subgroups. Consider for example the pseudo-algebraic functor $\mathcal{S}\ell_n$ over $\mathbb{Z}_p$. By functoriality of pseudo-algebraic groups, we have a morphism from $\mathcal{S}\ell_n(\mathbb{Z}_p)$ to $\mathcal{S}\ell_n(\mathbb{F}_p)$. Since both involved groups are profinite, the image of this morphism is a closed subgroup of $\mathcal{S}\ell_n(\mathbb{F}_p)$ and using the associated Lie rings it is possible to see that actually it is a closed proper subgroup. We may therefore wonder if this group is just infinite. Observe that in this case we can not adapt our proof of Theorem 0.2, as Proposition 6.10 — that holds for all pseudo-algebraic subgroups — fails.

The introduction of these other "Cartan type" groups is inspiring for another problem. Few computations should show, using Proposition 3.4, that the Hausdorff dimension of the special group over a finite field $\mathbb{F}_q$ — with respect to $\{\mathcal{G}\ell^i_n(\mathbb{F}_q)\}_{i\in\mathbb{N}}$ — is $(n-1)/n + 1/(np^n)$ (by the way, this value is not taken into account by Theorem 5.15). The appearance of $1/(np^n)$ is due to the fact that every pseudo-algebraic group (and thus every Cartan type group) contains the trivial pseudo-algebraic group, whereas — as we have just seen — the image of $\mathcal{S}\ell_n(\mathbb{Z}_p)$ does not.

Conjecture 2. Let $\mathcal{G}$ be a pseudo-algebraic functor over $\mathbb{Z}_p$ associated to an algebraic group of dimension $m \leq n$. Then the image of $\mathcal{G}(\mathbb{Z}_p)$ in $\mathcal{G}\ell_n(\mathbb{F}_p)$ has Hausdorff dimension — with respect to $\{\mathcal{G}\ell^i_n(\mathbb{F}_p)\}$ — equal to m/n.

Question 1. Let $\mathcal{G}$ be a pseudo-algebraic functor associated to an algebraic group of dimension m. Is there a formula depending only on p, m and n to compute its Hausdorff dimension?

About this question, notice that the Hausdorff dimension of the trivial pseudo-algebraic subgroup — computed in Section 5.2 — is $1/p^n$.

Finally, it might also be interesting to study what happens making the same construction of pseudo-algebraic subgroups changing the base algebra. For example, considering the automorphism group of some quotient of $R[\![\boldsymbol{t}]\!]$, or taking the total algebra on some monoid other than ${\mathbb{N}_0}^n$. In the first case we obtain groups related to subgroups defined in Section 5.1. In particular, dealing with $R[\![\boldsymbol{t}]\!]/\mathfrak{m}^2$ we obtain exactly the linear algebraic groups. We could even completely change the group $\mathrm{Aut}_{\mathfrak{m}}R[\![\boldsymbol{t}]\!]$. For example, groups constructed similarly to pseudo-algebraic subgroups can be obtained in the group of invertible germs in 0 of derivable functions $\mathbb{R}^n \to \mathbb{R}^n$.

Appendices

Appendix A

Inverse limits

Let $\mathcal{X} = \{X_\lambda,\ \pi_{\lambda\mu} : X_\mu \to X_\lambda,\ \Lambda\}$ be an inverse system of topological spaces (groups), in the notation of [33]. Using Bourbaki's convention [9] we define the inverse limit $\varprojlim \mathcal{X}$ of $\mathcal{X}$ to be

$$X := \{(x_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} X_\lambda \mid \pi_{\mu\lambda}(x_\lambda) = x_\mu \text{ for every } \lambda \geq \mu \in \Lambda\} \tag{A.1}$$

We denote π_λ the restriction of the canonical projection $\prod_{\lambda\in\Lambda} X_\lambda :\to X_\lambda$ to X.

Proposition A.1 (Universal property)**.** *Let Y be a topological space (group) and let $\{\rho_\lambda : Y \to X_\lambda \mid \lambda \in \Lambda\}$ be a family of continuous maps (homomorphisms) such that $\pi_{\lambda\mu} \circ \rho_\mu = \rho_\lambda$ whenever $\lambda \leq \mu$. Then there exists a unique continuous map (homomorphism) $\rho : Y \to X$ such that $\rho_\lambda = \pi_\lambda \circ \rho$.*

Proof. This might be considered a standard result. Bourbaki proves it [9, Chapter III, §7.2, Proposition 1] in the category of sets, but it can be easily extended in our setting. Otherwise the proof of [33, Proposition 1.1.1] also implies this proposition. □

Remark A.2. In [33] it is observed that the map $\mathcal{X} \mapsto \varprojlim \mathcal{X}$ is a functor from the category of inverse systems (see Section 1.1 of [33] for a definition of morphism of inverse systems) over topological spaces (groups) to the category of topological spaces (groups).

In what follows we assume that each X_λ is Hausdorff.

Proposition A.3 (Lemma 1.1.2 [33])**.** *The inverse limit of $\mathcal{X}$ is a closed subset of $\prod_\Lambda X_\lambda$.*

Proposition A.4. *Suppose $\Lambda = \mathbb{N}$ and each $\pi_{\lambda\mu}$ is surjective. then the projection $\pi_\lambda : \varprojlim \mathcal{X} \to X_\lambda$, that is the restriction to $\varprojlim \mathcal{X}$ of the canonical projection $\prod_{\nu\in\Lambda} X_\nu \to X_\lambda$, is surjective for every $\lambda \in \Lambda$. In particular $\varprojlim \mathcal{X}$ is not empty.*

Proof. Since, by our Definition (A.1), the forgetful functor from the category of topological space (groups) to sets preserves inverse limits, our claim follows from [9, Chapter III, §7.4, Proposition 5]. □

From now on, we assume that Λ is $\mathbb{N}$ and all maps $\pi_{\lambda\mu}$ are surjective.

Lemma A.5. *Every open neighbourhood O of any $x = (x_\lambda)_{\lambda\in\Lambda}$ in $\varprojlim \mathcal{X}$ contains $\pi_{\bar\lambda}^{-1}(x_{\bar\lambda})$ for some $\bar\lambda \in \Lambda$.*

Proof. Since we are considering the topology induced by $\prod_{\lambda\in\Lambda} X_\lambda$, the open neighbourhood O must contain $\varprojlim \mathcal{X} \cap \left(\prod_{\lambda\leq\bar\lambda} O_\lambda \times \prod_{\lambda>\bar\lambda} X_\lambda\right)$ for some $\bar\lambda \in \Lambda$, where each O_λ is an open neighbourhood of x_λ in X_λ. In particular

$$\varprojlim \mathcal{X} \cap \left(\prod_{\lambda<\bar\lambda} X_\lambda \times \{x_{\bar\lambda}\} \times \prod_{\lambda>\bar\lambda} X_\lambda\right) = \prod_{\lambda\leq\bar\lambda} \{x_\lambda\} \times \prod_{\lambda>\bar\lambda} \pi^{-1}_{\bar\lambda\lambda}(x_{\bar\lambda}) = \varprojlim \mathcal{X} \cap \left(\prod_{\lambda\leq\bar\lambda} \{x_\lambda\} \times \prod_{\lambda>\bar\lambda} X_\lambda\right)$$

is the preimage of $x_{\bar\lambda}$ through $\pi_{\bar\lambda}$ and it is contained in O. □

Proposition A.6. *Let S be a closed subset of $\varprojlim \mathcal{X}$. Then S equals $\varprojlim \mathcal{X} \cap \prod_{\lambda\in\Lambda} \pi_\lambda(S)$. In particular S is isomorphic to $\varprojlim \pi_\lambda(S)$.*

Proof. Clearly $S \subseteq \varprojlim \mathcal{X} \cap \prod_{\lambda\in\Lambda} \pi_\lambda(S)$. Let $s = (s_\lambda)_{\lambda\in\Lambda}$ be in $\varprojlim \mathcal{X} \cap \prod_{\lambda\in\Lambda} \pi_\lambda(S)$ and let O be an open neighbourhood of s in $\varprojlim \mathcal{X}$. Then O contains $\pi^{-1}_{\bar\lambda}(s_{\bar\lambda})$ that — since $s_{\bar\lambda} \in \pi_{\bar\lambda}(S)$ — in turn contains an element of S. Thus we proved that $\varprojlim \mathcal{X} \cap \prod_{\lambda\in\Lambda} \pi_\lambda(S)$ is contained in the closure of S, that is S itself, and so the claim follows. □

Appendix B

Combinatorial computations

Lemma B.1. *For every $a, b, c \in \mathbb{N}$*

$$\frac{(cb)^{n+1} - (ca-c))^{n+1}}{(n+1)!c} \leq \sum_{j=a}^{b} \binom{cj+n}{n} \leq \frac{(cb+n+c)^{n+1} - (ca+n)^{n+1}}{(n+1)!c}$$

and in particular $\sum_{j=a}^{b} \binom{j+n}{n}$ is asymptotic to $b^{n+1}/\left(c(n+1)!\right)$ as b tends to infinity.

Proof. First of all, we may observe that

$$\sum_{j=a}^{b} \binom{cj+n}{n} = \sum_{j=a}^{b} \frac{(cj+n)(cj+n-1)\cdots(cj+1)}{n!} \begin{cases} \leq \dfrac{1}{n!} \displaystyle\sum_{j=a}^{b} (cj+n)^n \\ \geq \dfrac{1}{n!} \displaystyle\sum_{j=a}^{b} (cj+1)^n \end{cases}$$

Since the function $\mathbb{R}_{\geq 0} \to \mathbb{R}$ that maps x to x^n is non-decreasing, we have that $c(cj+n)^n \leq \int_{cj+n}^{c(j+1)+n} x^n \mathrm{d}x$ and $c(cj+1)^n \geq \int_{c(j-1)+1}^{cj+1} x^n \mathrm{d}x$, whence

$$\sum_{j=a}^{b} \binom{cj+n}{n} \begin{cases} \leq \dfrac{1}{n!c} \displaystyle\int_{ca+n}^{c(b+1)+n} x^n \mathrm{d}x = \dfrac{1}{n!c} \left[\dfrac{x^{n+1}}{n+1}\right]_{ca+n}^{cb+c+n} \\ \geq \dfrac{1}{n!c} \displaystyle\int_{c(a-1)+1}^{cb+1} x^n \mathrm{d}x = \dfrac{1}{n!c} \left[\dfrac{x^{n+1}}{n+1}\right]_{c(a-1)}^{cb} \end{cases}$$

yielding the claim. □

Remark B.2. Actually it can be easily proved — by induction or using Lemma 1.2 — that $\sum_{j=a}^{b} \binom{j+n}{n}$ is exactly $\binom{b+n+1}{n+1} - \binom{a+n}{n+1}$.

Lemma B.3. *Let p be a prime. The product of all elements of the multiplicative group of a finite field of order p equals -1. In other words: $\prod_{i=1}^{p-1} i \equiv_p -1$.*

Proof. All elements of the field satisfy the equation $T^p - T = 0$. In particular, all non-null elements satisfy $T^{p-1} - 1 = 0$. Therefore $\prod_{a \in \mathbb{F}_p^\times} (T-a) = T^{p-1} - 1$, whence

$$\prod_{a \in \mathbb{F}_p^\times} a = (-1)^{p-1} \prod_{a \in \mathbb{F}_p^\times} a = \prod_{a \in \mathbb{F}_p^\times} (-a) = -1$$

□

We recall that, by convention, the binomial coefficient $\binom{a}{b}$ is equal to zero whenever $a < b$.

Lemma B.4. *Let p be a prime and $a \geq b$ be positive integers whose p-adic expansions are $\sum_{i=0}^{r} a_i p^i$ and $\sum_{i=0}^{s} b_i p^i$ respectively, where $\lfloor \log_p b \rfloor = s \leq r = \lfloor \log_p a \rfloor$ and $a_i, b_i \in \{0, \dots, p-1\}$ for every i. Then $\binom{a}{b} \equiv_p \prod_{i=0}^{r} \binom{a_i}{b_i}$ where we assume b_i to be zero whenever $i > s$.*

Proof. All along this proof, for every non-negative integer x, the symbol $\{x\}$ denotes some — we do not care which one — non-negative integer equivalent to x modulo p.

First assume $b = b_1 p + b_0$ and $a = a_1 p + a_0$ for some non-negative integers b_1, a_1, b_0, a_0 such that $b_0, a_0 < p$. Then

$$a! = (a_1 p + a_0)(a_1 p + a_0 - 1) \cdots (a_1 p + 1)(a_1 p)! = \{a_0!\}(a_1 p)!$$

with $(a_1 p)!$ that equals

$$a_1 p \underbrace{(a_1 p - 1) \cdots (a_1 p - p + 1)}_{(*)} (a_1 - 1) p \underbrace{(a_1 p - p - 1) \cdots (a_1 p - 2p + 1)}_{(*)} (a_1 - 2) p \cdots p \underbrace{(p-1)!}_{(*)}$$

where each product denoted by $(*)$ is equivalent to -1 modulo p. Therefore

$$(a_1 p)! = a_1! p^{a_1} \{(-1)^{a_1}\}$$

and analogous results hold for b. It follows, if $a_0 \geq b_0$ — since $a - b = (a_1 - b_1)p + (a_0 - b_0)$ —

$$\binom{a}{b} = \frac{\{a_0!\} a_1! p^{a_1} \{(-1)^{a_1}\}}{\{b_0!\} b_1! p^{b_1} \{(-1)^{b_1}\} \{(a_0 - b_0)!\} (a_1 - b_1)! p^{a_1 - b_1} \{(-1)^{a_1 - b_1}\}} \equiv_p \binom{a_0}{b_0} \binom{a_1}{b_1} \tag{B.1}$$

On the other hand, if $b_0 > a_0$, then we write $a - b$ as $(a_1 - b_1 - 1)p + p + a_0 - b_0$, obtaining

$$\begin{aligned}\binom{a}{b} &= \frac{\{a_0!\} a_1! p^{a_1} \{(-1)^{a_1}\}}{\{b_0!\} b_1! p^{b_1} \{(-1)^{b_1}\} \{(p + a_0 - b_0)!\} (a_1 - b_1 - 1)! p^{a_1 - b_1 - 1} \{(-1)^{a_1 - b_1 - 1}\}} \\ &= \frac{p \{a_0!\} a_1! \{(-1)\}}{\{b_0!\} b_1! \{(p + a_0 - b_0)!\} (a_1 - b_1 - 1)!} = p(a_1 - b_1) \binom{a_1}{b_1} \frac{\{a_0!\}}{\{b_0!\}\{(p + a_0 - b_0)!\}} \equiv_p 0\end{aligned}$$

that is obviously equivalent to $\binom{a_0}{b_0}\binom{a_1}{b_1}$.

Thus we may proceed by induction on r to prove the statement. □

Corollary B.5. *Let p be a prime and fix three positive integers a, b and s. Then $\binom{ap^s}{b} \equiv_p 0$ unless $b = p^s b'$ for some $b' \in \mathbb{N}_0$ and in that case $\binom{ap^s}{b' p^s} \equiv_p \binom{a}{b'}$.*

Corollary B.6. *Let p be a prime and R be an algebra over the finite field of order p. Fix a positive integer s. For every $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$, and every $f \in R[\![\boldsymbol{t}]\!]$, we have*

$$\partial_{\boldsymbol{\alpha}} \left(f^{p^s} \right) = (\partial_{\boldsymbol{\alpha}'} f)^{p^s}$$

if there exists $\boldsymbol{\alpha}' \in {\mathbb{N}_0}^n$ such that $\boldsymbol{\alpha} = p^s \boldsymbol{\alpha}'$, otherwise it is 0.

Corollary B.7. *Let p be a prime and a, b, l non negative integers such that both a and b are less than p^{l+1}, but $a + b$ is not. Then $\binom{a+b}{a} \equiv_p 0$.*

A proof of this last corollary may be found in [38, Lemma 3.5.8], however we give an other version relying on previous results.

Proof. Let $a = a_0+a_1p+\dots a_lp^l$, $b = b_0+b_1p+\dots b_lp^l$ and $a+b = (a+b)_0+(a+b)_1p+\dots(a+b)_mp^m$ be the p-adic expansions of a, b and $a+b$ respectively (of course $m > l$, actually $m = l+1$). By hypothesis there exists $i \leq l$ such that $a_i + b_i > p$ and therefore $(a+b)_i = a_i + b_i - p \leq a_i$. Thus $\binom{(a+b)_i}{a_i} = 0$ and the claim follows from Lemma B.4. □

Lemma B.8. *Let R be an $\mathbb{F}_p$-algebra for some prime p. Let l be a positive integer and let $\boldsymbol{\alpha} \in {\mathbb{N}_0}^n$ be such that $\boldsymbol{\alpha} \leq (p^l-1)\mathbf{1}$. Then $\partial_{\boldsymbol{\alpha}} f^{p^l} g = f^{p^l}\partial_{\boldsymbol{\alpha}} g$ for every $f, g \in R[\![\boldsymbol{t}]\!]$.*

Proof. For every $\boldsymbol{\gamma} \in {\mathbb{N}_0}^n$, let $\boldsymbol{\gamma}_0 \leq (p^l-1)\mathbf{1}$ and $\boldsymbol{\gamma}_1$ be such that $\boldsymbol{\gamma} = p^l\boldsymbol{\gamma}_1 + \boldsymbol{\gamma}_0$. Then, by Lemma B.4, we have

$$\partial_{\boldsymbol{\alpha}}(\boldsymbol{t}^{p^l\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\gamma}}) = \binom{\boldsymbol{\gamma}_1+\boldsymbol{\beta}}{0}\binom{\boldsymbol{\gamma}_0}{\boldsymbol{\alpha}}\boldsymbol{t}^{p^l\boldsymbol{\beta}+\boldsymbol{\gamma}-\boldsymbol{\alpha}} = \boldsymbol{t}^{p^l\boldsymbol{\beta}}\binom{\boldsymbol{\gamma}_1}{0}\binom{\boldsymbol{\gamma}_0}{\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\gamma}-\alpha} = \boldsymbol{t}^{p^l\boldsymbol{\beta}}\partial_{\boldsymbol{\alpha}}\boldsymbol{t}^{\boldsymbol{\gamma}}$$

for every $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$. So the claim follows from $\mathbb{F}_p$-linearity of the map $f \in R[\![\boldsymbol{t}]\!] \mapsto f^{p^l} \in R[\![\boldsymbol{t}]\!]$. □

Lemma B.9. *Let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be in ${\mathbb{N}_0}^n$. Then for every $f \in R[\![\boldsymbol{t}]\!]$, we have $\partial_{\boldsymbol{\alpha}}\partial_{\boldsymbol{\beta}} f = \binom{\boldsymbol{\alpha}+\boldsymbol{\beta}}{\boldsymbol{\beta}}\partial_{\boldsymbol{\alpha}+\boldsymbol{\beta}} f$.*

Proof. It suffices to prove the statement for $f = \boldsymbol{t}^{\boldsymbol{\gamma}}$ for any $\boldsymbol{\gamma} \in {\mathbb{N}_0}^n$. Thus

$$\partial_{\boldsymbol{\alpha}}\partial_{\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\gamma}} = \partial_{\boldsymbol{\alpha}}\binom{\boldsymbol{\gamma}}{\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\gamma}-\boldsymbol{\beta}} = \binom{\boldsymbol{\gamma}-\boldsymbol{\beta}}{\boldsymbol{\alpha}}\binom{\boldsymbol{\gamma}}{\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\gamma}-\boldsymbol{\alpha}-\boldsymbol{\beta}}$$

where one might check that

$$\binom{\boldsymbol{\gamma}-\boldsymbol{\beta}}{\boldsymbol{\alpha}}\binom{\boldsymbol{\gamma}}{\boldsymbol{\beta}} = \binom{\boldsymbol{\alpha}+\boldsymbol{\beta}}{\boldsymbol{\alpha}}\binom{\boldsymbol{\gamma}}{\boldsymbol{\alpha}+\boldsymbol{\beta}}$$

so that, by definition, $\partial_{\boldsymbol{\alpha}}\partial_{\boldsymbol{\beta}}\boldsymbol{t}^{\boldsymbol{\gamma}} = \binom{\boldsymbol{\alpha}+\boldsymbol{\beta}}{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}+\boldsymbol{\beta}} f$ as requested. □

Corollary B.10. *For every $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ in ${\mathbb{N}_0}^n$, the maps $\partial_{\boldsymbol{\alpha}}$ and $\partial_{\boldsymbol{\beta}}$ commute.*

Corollary B.11. *Let p be a prime and assume R is an $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$-algebra. Let s be a positive integer. Then, for every $\boldsymbol{\alpha} \leq (p^s-1)\mathbf{1}$ and every $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$. We have $\partial_{p^s\boldsymbol{\beta}}\partial_{\boldsymbol{\alpha}} = \partial_{p^s\boldsymbol{\beta}+\boldsymbol{\alpha}}$.*

Proof. It is a simple consequence of Lemma B.9 and Lemma B.4. □

Corollary B.12. *Let p be a prime and assume R is an $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$-algebra. Let l be a positive integer and $\boldsymbol{\alpha}, \boldsymbol{\beta} \in {\mathbb{N}_0}^n$ be such that both of them are less than $(p^l-1)\mathbf{1}$, but their sum is not. Then $\partial_{\boldsymbol{\alpha}}\partial_{\boldsymbol{\beta}} f = 0$ for every $f \in R[\![\boldsymbol{t}]\!]$.*

Proof. By Lemma B.9 we have

$$\partial_{\boldsymbol{\alpha}}\partial_{\boldsymbol{\beta}} = \binom{\boldsymbol{\alpha}+\boldsymbol{\beta}}{\boldsymbol{\alpha}}\partial_{\boldsymbol{\alpha}+\boldsymbol{\beta}}$$

that is zero because of Corollary B.7. □

Corollary B.13. *Let p be a prime and assume R is an $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$-algebra. Let $\boldsymbol{\alpha}_1, \dots, \boldsymbol{\alpha}_m \in {\mathbb{N}_0}^n$ — where $m > 1$ — and $l \in \mathbb{N}$ be such that $\boldsymbol{\alpha}_i \leq (p^l-1)\mathbf{1}$ for every $1 \leq i \leq m$, but $\sum_{i=1}^m \boldsymbol{\alpha}_i \not\leq (p^l-1)\mathbf{1}$. Then $\partial_{\boldsymbol{\alpha}_1}\partial_{\boldsymbol{\alpha}_2}\dots\partial_{\boldsymbol{\alpha}_m} f = 0$ for every $f \in R[\![\boldsymbol{t}]\!]$.*

Proof. Let $j \leq n$ be such that $\sum_{i=1}^{j} \boldsymbol{\alpha}_i \leq (p^l - 1)\mathbf{1}$ but $\sum_{i=1}^{j+1} \boldsymbol{\alpha}_i \not\leq (p^l - 1)\mathbf{1}$. Because of the Lemma B.9, we have

$$\partial_{\boldsymbol{\alpha}_1} \partial_{\boldsymbol{\alpha}_2} \dots \partial_{\boldsymbol{\alpha}_m} f = c \partial_{\boldsymbol{\alpha}_1 + \dots + \boldsymbol{\alpha}_j} \partial_{\boldsymbol{\alpha}_{j+1}} \dots \partial_{\boldsymbol{\alpha}_m} f$$

where c is some positive integer integer and $\partial_{\boldsymbol{\alpha}_1 + \dots + \boldsymbol{\alpha}_j} \partial_{\boldsymbol{\alpha}_{j+1}}$ is the zero R-linear endomorphism because of the previous corollary. □

Lemma B.14. *Let x, w be non-negative integers. For every $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$ of weight $x(w + n - 1)$ there exists $\boldsymbol{\alpha}$ of weight w such that $x\boldsymbol{\alpha} \leq \beta$.*

Proof. If $w = 0$ the claim is trivial. Assume $w = 1$. Then for every $\boldsymbol{\beta} = (\beta_i)_{i=1}^n$ of weight $x(1 + n - 1) = nx$ there exists $j \in \{1, \dots, n\}$ such that $\beta_j \geq x$ and therefore $x\boldsymbol{\epsilon}_j \leq \boldsymbol{\beta}$. Now we proceed by induction. Let w be greater than 1. Then, by inductive hypothesis, for every $\boldsymbol{\beta} \in {\mathbb{N}_0}^n$ of weight $x(w + n - 1)$ there exists $\boldsymbol{\alpha}_1 \in {\mathbb{N}_0}^n$ of weight $w - 1 \geq 1$ such that $x\boldsymbol{\alpha}_1 \leq \boldsymbol{\beta}$. Thus $\boldsymbol{\beta} - x\boldsymbol{\alpha}_1$ has weight $x(1 + n - 1)$ and applying again inductive hypothesis there exists $\boldsymbol{\alpha}_2 \in {\mathbb{N}_0}^n$ of weight 1 such that $x\boldsymbol{\alpha}_2 \leq \boldsymbol{\beta} - x\boldsymbol{\alpha}_1$. Thus $\boldsymbol{\alpha} = \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2$ satisfies our requirements. □

Appendix C

Miscellanea

Proposition C.1. *Let H be an abstract group endowed with a topology such that there is a family of open normal subgroups $\{H_i\}_{i\in i}$ that form a base for the neighbourhoods of 1. Then H is a topological group.*

Proof. Let g and h be in H. Then any open neighbourhood of gh (resp. g^{-1}) contains ghH_i (resp. $g^{-1}H_i$) for some $i \in I$ and $gH_i \times hH_i$ (resp. gH_i) is an open neighbourhood of $(g, h) \in H \times H$ (resp. $g \in H$) whose image is contained — indeed they coincides — in ghH_i (resp. $g^{-1}H_i$). □

Lemma C.2. *Let G be a topological group and $\{G_i\}$ an N-series. Then for every $i, j, l \in \mathbb{N}$, every f, g, h in G_i, G_j, G_l respectively,*

$$r := \left[\left[f, g\right], h\right]\left[\left[g, h\right], f\right]\left[\left[h, f\right], g\right] \in G_{i+j+l+1}$$

is in $G_{i+j+l+1}$.

Proof. By direct computations

$$\begin{aligned} r = [g, f]\,[fh, g]\,[gf, h]\,[h, f]^g &= [g, f]\,[gf, h]\,[fh, g]\,[[fh, g]\,, [gf, h]]\,[h, f]^g = \\ &= \underbrace{[g, f]\,[gf, h]\,[fh, g]\,[h, f]^g}_{(*)}\underbrace{[[fh, g]\,, [gf, h]]\,[[[fh, g]\,, [gf, h]]\,, [h, f]^g]}_{(**)} \end{aligned}$$

where one can verify that $(*) = 1$, whereas $(**) \in G_{\min\{i,l\}+j+\min\{j,i\}+i}$.

If $i \ngtr \max\{j, l\}$ then the claim follows immediately. Otherwise, since $G_{i+j+l}/G_{i+j+l+1}$ is commutative, we have

$$r \equiv \left[\left[g, h\right], f\right]\left[\left[h, f\right], g\right]\left[\left[f, g\right], h\right] \mod G_{i+j+l+1}$$

and we can repeat the same computations shifting f, g, h. □

Lemma C.3 (Lemma 9 [39])**.** *Let G be a pro-p group with open normal subgroups G_i, M_i with $i \in \mathbb{N}$ such that the following statements hold.*

(1) The sequence G_i is a filtration of G.

(2) $G_i > M_i$ for all $i \in \mathbb{N}$.

(3) The factors G_i/M_i are elementary abelian p-groups for all $i \in \mathbb{N}$.

(4) The images of the group elements are linearly independent under the natural map

$$\begin{aligned}\sigma : G \mapsto & \mathrm{End}_{\mathbb{F}_p}\left(\bigoplus_{i\geq k} G_i/M_i\right)\\ g \mapsto & \big(\sigma(g) : (v_k, v_{k+1}, \ldots) \mapsto (v_k^g, v_{k+1}^g, \ldots)\big)\end{aligned}$$

for all natural numbers k.

Then d random elements of G, for any positive integer d, generate a free group of rank d with probability 1.

Before proving the lemma, we have to make some observation. Let w_0 be a word in the free group F of rank r generated by $x_1, \ldots, x_r$. Then it is possible to show by induction on the length of w_0 that there exists a positive integer s, a sequence $(j_i)_{i=1}^s \in \{1, \ldots, r\}^s$, a sequence $(\varepsilon_i)_{i=1}^s \in \{-1, 1\}^s$ and words w_i and z_i in F such that $w_{i-1} = z_i w_i$ for every $1 \leq i \leq s$ with the following property: for every group homomorphism $\phi : F \to G$ such that $\phi(x_i) = a_i b_i$ for some $a_1, \ldots, a_r, b_1, \ldots, b_r \in G$, we have

$$\phi(w) = \tilde{\phi}(w) \prod_{i=1}^{s} ({b_{j_1}}^{\varepsilon_i})^{\tilde{\phi}(w_i)} \tag{C.1}$$

where $\tilde{\phi}$ is the homomorphism $F \to G$ such that $\tilde{\phi}(x_i) = a_i$ for every $1 \leq i \leq r$.

We can now face the proof of Lemma C.3.

Proof. Let S_w denotes the set of d-tuples $(a_i)_{i=1}^d$ in G^d that satisfy the equation $w(a_1, \ldots, a_d) = 1$. We want to prove that for any word w in the free group $F(x_1, \ldots, x_d)$ generated by $x_1, \ldots, x_d$, the equation $w(a_1, \ldots, a_d) = 1$ is satisfied with probability 0 in G^d. The claim then follows, since the set of d-tuples in G^d that do not generate a free group of rank d is $\bigcup_{w\in F(x_1\ldots,x_d)} S_w$, that is the union of countably many null sets and therefore it has measure 0.

So, assume it is not the case, that is to say there exists a reduced word $w \in F(x_1, \ldots, x_n)$ such that $\mu_{G^d}(\{(a_i)_{i=1}^d \in G^d \mid w(a_1, \ldots, a_d) = 1\}) = \varepsilon > 0$. We may also assume that w is minimal, i. e. for every word s of length less than the length of w the set of d-tuples $(a_i)_{i=1}^d$ in G^d such that $s(a_1, \ldots, a_n) = 1$ has measure 0. Then the set

$$H := S_w \setminus \left(\bigcup_{l(s)<l(w)} S_s\right)$$

— where l denotes the length function — has positive measure. By [39, Proposition 7], there exists a d-tuple $(a_i)_{i=1}^d$ in G^d and a positive integer k such that

$$\frac{\mu_{G^d}(H \cap (a_i G_j)_{i=1}^n)}{\mu_{G^d}((a_i G_j)_{i=1}^n)} > 1/p \tag{C.2}$$

for every $j \geq k$.

For every positive integer j consider the map $\phi_j : (G_j/M_j)^d \to (G_j/M_j)$ that maps each $(v_1 M_j, \ldots, v_d M_j) \in (G_j/M_j)^d$ to $w(a_1 v_1 M_j, \ldots, a_d v_d M_j)$. Since $w(a_1, \ldots, a_d)$ is trivial, the subgroup G_j is normal in G and G_j/M_j is elementary abelian, by equation (C.1) the map ϕ_j is $\mathbb{F}_p$-linear.

On the other hand, equation (C.1) also implies that $w(a_1 v, a_2, \ldots, a_d) = \prod_{i=1}^s (v^{\varepsilon_i})^{w_i(a_1,\ldots,a_d)}$ for some $s \in \mathbb{N}_0$, some terminal subwords w_i $(1 \leq i \leq s)$ and some sequence of $(\varepsilon_i)_{i=1}^n \in \{-1, 1\}^s$.

So $\phi_j(vM_j, M_j, \dots, M_j)$ equals the image of v through the endomorphism of G_j/M_j given by $\sum_{i=1}^{s} \varepsilon_i \sigma(w_i(a_1, \dots, a_d))$. Moreover we may assume without loss of generality that w has length greater than 1 and starts with x_1, so that there exists at least one non trivial word w_i, and that all words w_i are distinct — otherwise there would be consecutive occurrences of v (or v^{-1}) in the expression of $w(a_1 v, a_2, \dots, a_d)$ — and therefore so they are the corresponding elements $w_i(a_1, \dots, a_d)$ in G by definition of H. By hypothesis there exists $j > k$ and $v \in G_j$ such that its image through $\sum_{i=1}^{s} \varepsilon_i \sigma(w_i(a_1, \dots, a_d))$ is not trivial, i. e. the map ϕ_j is not trivial. Then its kernel K has codimension at least 1 and therefore $|G_j/M_j : K| \geq p$. Since $K = (a_i^{-1})_{i=1}^{n} \left(H \cap (a_i G_j)_{i=1}^{n}\right) / M_j$, this implies $\mu_{G^d}\left(H \cap (a_i G_j)_{i=1}^{n}\right) \leq \frac{1}{p} \mu_{G^d}((a_i G_j)_{i=1}^{n})$, contradicting inequality (C.2). □

Index

$\partial_{\boldsymbol{\beta}}$, 10
∂_i, 17
$\circ$, 5
$\mathit{\Psi}$, 46
$\omega\,(\boldsymbol{f})$, 10

$\mathsf{A}\,(l,\ \boldsymbol{\omega},\ \boldsymbol{f},\ d_0)$, 47
admissible index-set, 38
associated Lie ring, 18
$\mathrm{Aut}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$, 7
$\mathrm{Aut}^i_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$, 7

contact algebra, 25
contact group, 25

dense$\,(I)$, 41
density, 41
depth, 10
$\mathrm{Der}_R\,(A)$, 17
$\mathrm{Der}^j_R\,(R[\![\boldsymbol{t}]\!])$, 17
derivation, 17
div, 25
divergence, 25
$\mathsf{D}\,(s,\ \boldsymbol{\chi})$, 46

$\boldsymbol{E}_i$, 9
$\mathrm{End}_{\mathfrak{m}} R[\![\boldsymbol{t}]\!]$, 5

$\lceil f \rceil$, 20
$\mathbb{F}_q$, vii
filtration, 18
formal partial derivative, 17

$\mathcal{GL}^i_n\,(R)$, 8

$\mathcal{H}^1{}_n\,(R)$, 25
$H_n(R)$, 25
hamiltonian algebra, 25
hamiltonian group, 25
Hausdorff dimension, vii
Hausdorff spectrum, vii, 38
hom_i, 17

Hopf algebra, 28

index-subgroups, 38

$\mathcal{J}(I)$, 38
Jac$(\boldsymbol{f})$, 9
Jacobian matrix, 9

$\mathcal{K}\,(I)$, 36
$\mathcal{K}^1{}_n\,(R)$, 25
$K_n(R)$, 25

$L(G)$, 18
$L_G(H)$, 19
ldense$\,(I)$, 40
Lie$\,(\mathcal{G})$, 34
linear algebraic group, 29
lower density, 40

$\mathcal{M}_n(R)$, 5
$\mathfrak{m}$, 4
$\mathcal{M}^i_n(R)$, 5
$\mathfrak{m}$, 4

$\mathbb{N}$, vii
N-series, 18
$\mathbb{N}_0$, vii
$\mathbb{N}_0{}^n$, 3
N_p-series, 18
Nottingham group, 8

ord$\,(f)$, 4
order, 4, 10
ord$\,(\boldsymbol{f})$, 10

pseudo-algebraic functor, 33
pseudo-algebraic group, 30

$\mathbb{Q}$, vii

R, 2
$\mathbb{R}$, vii

restricted d-support, 38
$R[\![\boldsymbol{t}]\!]$, 4
$(R[\![\boldsymbol{t}]\!])^n$, 5

$S_n(R)$, 25
$\mathsf{S}\,(l,\ D)$, 46
$\mathcal{Sl}^1{}_n\,(R)$, 25
special algebra, 25
special group, 25
$\mathcal{St}\,(I)$, 36
substitution, 5
Supp$\boldsymbol{f}$, 38
Supp$f$, 38
Supp$_d\boldsymbol{f}$, 38
support, 38

$\boldsymbol{t}$, 9

udense$\,(I)$, 40
upper density, 40

$\mathbb{Z}$, vii
$\mathbb{Z}_p$, vii

Bibliography

[1] A. G. Abercrombie. “Subgroups and subrings of profinite rings”. In: *Math. Proc. Cambridge Philos. Soc.* 116.2 (1994), pp. 209–222. ISSN: 0305-0041. DOI: 10.1017/S0305004100072522. URL: https://doi.org/10.1017/S0305004100072522.

[2] Y. Barnea, M. Ershov, and T. Weigel. “Abstract commensurators of profinite groups”. In: *Trans. Amer. Math. Soc.* 363.10 (2011), pp. 5381–5417. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-2011-05295-5. URL: https://doi.org/10.1090/S0002-9947-2011-05295-5.

[3] Y. Barnea and B. Klopsch. “Index-subgroups of the Nottingham group”. In: *Adv. Math.* 180.1 (2003), pp. 187–221. ISSN: 0001-8708. DOI: 10.1016/S0001-8708(02)00102-0. URL: https://doi.org/10.1016/S0001-8708(02)00102-0.

[4] Y. Barnea and A. Shalev. “Hausdorff dimension, pro-p groups, and Kac-Moody algebras”. In: *Trans. Amer. Math. Soc.* 349.12 (1997), pp. 5073–5091. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-97-01918-1. URL: https://doi.org/10.1090/S0002-9947-97-01918-1.

[5] Y. Barnea et al. “Pro-p groups with few normal subgroups”. In: *J. Algebra* 321.2 (2009), pp. 429–449. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2008.10.012. URL: https://doi.org/10.1016/j.jalgebra.2008.10.012.

[6] R. E. Block and R.L. Wilson. “Classification of the restricted simple Lie algebras”. In: *J. Algebra* 114.1 (1988), pp. 115–259. ISSN: 0021-8693. DOI: 10.1016/0021-8693(88)90216-5. URL: https://doi.org/10.1016/0021-8693(88)90216-5.

[7] N. Bourbaki. *Algebra II. Chapters 4–7.* Elements of Mathematics (Berlin). Translated from the 1981 French edition by P. M. Cohn and J. Howie, Reprint of the 1990 English edition [Springer, Berlin; MR1080964 (91h:00003)]. Springer-Verlag, Berlin, 2003, pp. viii+461. ISBN: 3-540-00706-7. DOI: 10.1007/978-3-642-61698-3. URL: https://doi.org/10.1007/978-3-642-61698-3.

[8] N. Bourbaki. *Elements of mathematics. Algebra, Part I: Chapters 1-3.* Translated from the French. Hermann, Paris; Addison-Wesley Publishing Co., Reading Mass., 1974, pp. xxiii+709.

[9] N. Bourbaki. *Theory of sets.* Elements of Mathematics (Berlin). Reprint of the 1968 English translation [Hermann, Paris; MR0237342]. Springer-Verlag, Berlin, 2004, pp. viii+414. ISBN: 3-540-22525-0. DOI: 10.1007/978-3-642-59309-3. URL: https://doi.org/10.1007/978-3-642-59309-3.

[10] R. Camina. “Subgroups of the Nottingham group”. In: *J. Algebra* 196.1 (1997), pp. 101–113. ISSN: 0021-8693. DOI: 10.1006/jabr.1997.7082. URL: https://doi.org/10.1006/jabr.1997.7082.

[11] R. Camina. "The Nottingham group". In: *New horizons in pro-p groups.* Vol. 184. Progr. Math. Birkhäuser Boston, Boston, MA, 2000, pp. 205–221.

[12] C. Chevalley. "On the theory of local rings". In: *Ann. of Math. (2)* 44 (1943), pp. 690–708. ISSN: 0003-486X. DOI: 10.2307/1969105. URL: https://doi.org/10.2307/1969105.

[13] S. Donkin. "Space groups and groups of prime-power order. VIII. Pro-p-groups of finite coclass and p-adic Lie algebras". In: *J. Algebra* 111.2 (1987), pp. 316–342. ISSN: 0021-8693. DOI: 10.1016/0021-8693(87)90219-5. URL: https://doi.org/10.1016/0021-8693(87)90219-5.

[14] M. Ershov. "New just-infinite pro-p groups of finite width and subgroups of the Nottingham group". In: *J. Algebra* 275.1 (2004), pp. 419–449. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2003.08.012. URL: https://doi.org/10.1016/j.jalgebra.2003.08.012.

[15] M. Ershov. "On the commensurator of the Nottingham group". In: *Trans. Amer. Math. Soc.* 362.12 (2010), pp. 6663–6678. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-2010-05160-8. URL: https://doi.org/10.1090/S0002-9947-2010-05160-8.

[16] M. V. Ershov. "The Nottingham group is finitely presented". In: *J. London Math. Soc. (2)* 71.2 (2005), pp. 362–378. ISSN: 0024-6107. DOI: 10.1112/S0024610704006131. URL: https://doi.org/10.1112/S0024610704006131.

[17] K. Falconer. *Fractal geometry.* Second. Mathematical foundations and applications. John Wiley & Sons, Inc., Hoboken, NJ, 2003, pp. xxviii+337. ISBN: 0-470-84861-8. DOI: 10.1002/0470013850. URL: https://doi.org/10.1002/0470013850.

[18] I. Fesenko. "On just infinite pro-p-groups and arithmetically profinite extensions of local fields". In: *J. Reine Angew. Math.* 517 (1999), pp. 61–80. ISSN: 0075-4102. DOI: 10.1515/crll.1999.098. URL: https://doi.org/10.1515/crll.1999.098.

[19] R. I. Grigorchuk. "Just infinite branch groups". In: *New horizons in pro-p groups.* Vol. 184. Progr. Math. Birkhäuser Boston, Boston, MA, 2000, pp. 121–179.

[20] P. Hegedűs. "The Nottingham group for $p = 2$". In: *J. Algebra* 246.1 (2001), pp. 55–69. ISSN: 0021-8693. DOI: 10.1006/jabr.2001.8948. URL: https://doi.org/10.1006/jabr.2001.8948.

[21] D. L. Johnson. "The group of formal power series under substitution". In: *J. Austral. Math. Soc. Ser. A* 45.3 (1988), pp. 296–302. ISSN: 0263-6115.

[22] B. Klopsch. "Automorphisms of the Nottingham group". In: *J. Algebra* 223.1 (2000), pp. 37–56. ISSN: 0021-8693. DOI: 10.1006/jabr.1999.8040. URL: https://doi.org/10.1006/jabr.1999.8040.

[23] C. R. Leedham-Green. "Pro-p-groups of finite coclass". In: *J. London Math. Soc. (2)* 50.1 (1994), pp. 43–48. ISSN: 0024-6107. DOI: 10.1112/jlms/50.1.43. URL: https://doi.org/10.1112/jlms/50.1.43.

[24] C. R. Leedham-Green. "The structure of finite p-groups". In: *J. London Math. Soc. (2)* 50.1 (1994), pp. 49–67. ISSN: 0024-6107. DOI: 10.1112/jlms/50.1.49. URL: https://doi.org/10.1112/jlms/50.1.49.

[25] C. R. Leedham-Green and S. McKay. *The structure of groups of prime power order.* Vol. 27. London Mathematical Society Monographs. New Series. Oxford Science Publications. Oxford University Press, Oxford, 2002, pp. xii+334. ISBN: 0-19-853548-1.

[26] C. R. Leedham-Green, S. McKay, and W. Plesken. “Space groups and groups of prime power order. VI. A bound to the dimension of a 2-adic space group with fixed coclass”. In: *J. London Math. Soc. (2)* 34.3 (1986), pp. 417–425. ISSN: 0024-6107. DOI: 10.1112/jlms/s2-34.3.417. URL: https://doi.org/10.1112/jlms/s2-34.3.417.

[27] C. R. Leedham-Green, S. McKay, and W. Plesken. “Space groups and groups of prime-power order. V. A bound to the dimension of space groups with fixed coclass”. In: *Proc. London Math. Soc. (3)* 52.1 (1986), pp. 73–94. ISSN: 0024-6115. DOI: 10.1112/plms/s3-52.1.73. URL: https://doi.org/10.1112/plms/s3-52.1.73.

[28] C. R. Leedham-Green and M. F. Newman. “Space groups and groups of prime-power order. I”. In: *Arch. Math. (Basel)* 35.3 (1980), pp. 193–202. ISSN: 0003-889X. DOI: 10.1007/BF01235338. URL: https://doi.org/10.1007/BF01235338.

[29] R. Pink. “Compact subgroups of linear algebraic groups”. In: *J. Algebra* 206.2 (1998), pp. 438–504. ISSN: 0021-8693. DOI: 10.1006/jabr.1998.7439. URL: https://doi.org/10.1006/jabr.1998.7439.

[30] C. D. Reid. “Inverse system characterizations of the (hereditarily) just infinite property in profinite groups”. In: *Bull. Lond. Math. Soc.* 44.3 (2012), pp. 413–425. ISSN: 0024-6093. DOI: 10.1112/blms/bdr099. URL: https://doi.org/10.1112/blms/bdr099.

[31] C. D. Reid. *Inverse system characterizations of the (hereditarily) just infinite property in profinite groups.* 2017. arXiv: 1708.08301 [math.GR].

[32] C. D. Reid. “On the structure of just infinite profinite groups”. In: *J. Algebra* 324.9 (2010), pp. 2249–2261. ISSN: 0021-8693. DOI: 10.1016/j.jalgebra.2010.07.034. URL: https://doi.org/10.1016/j.jalgebra.2010.07.034.

[33] L. Ribes and P. Zalesskii. *Profinite groups.* Second. Vol. 40. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]. Springer-Verlag, Berlin, 2010, pp. xvi+464. ISBN: 978-3-642-01641-7. DOI: 10.1007/978-3-642-01642-4. URL: https://doi.org/10.1007/978-3-642-01642-4.

[34] A. Shalev. “Finite p-groups”. In: *Finite and locally finite groups (Istanbul, 1994).* Vol. 471. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. Kluwer Acad. Publ., Dordrecht, 1995, pp. 401–450.

[35] A. Shalev. “Lie methods in the theory of pro-p groups”. In: *New horizons in pro-p groups.* Vol. 184. Progr. Math. Birkhäuser Boston, Boston, MA, 2000, pp. 1–54.

[36] A. Shalev. “The structure of finite p-groups: effective proof of the coclass conjectures”. In: *Invent. Math.* 115.2 (1994), pp. 315–345. ISSN: 0020-9910. DOI: 10.1007/BF01231763. URL: https://doi.org/10.1007/BF01231763.

[37] A. Shalev and E. I. Zel′manov. “Pro-p groups of finite coclass”. In: *Math. Proc. Cambridge Philos. Soc.* 111.3 (1992), pp. 417–421. ISSN: 0305-0041. DOI: 10.1017/S0305004100075514. URL: https://doi.org/10.1017/S0305004100075514.

[38] H. Strade and R. Farnsteiner. *Modular Lie algebras and their representations.* Vol. 116. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1988, pp. x+301. ISBN: 0-8247-7594-5.

[39] B. Szegedy. “Almost all finitely generated subgroups of the Nottingham group are free”. In: *Bull. London Math. Soc.* 37.1 (2005), pp. 75–79. ISSN: 0024-6093. DOI: 10.1112/S0024609304003972. URL: https://doi.org/10.1112/S0024609304003972.

[40] M. Vannacci. “On hereditarily just infinite profinite groups obtained via iterated wreath products”. In: *J. Group Theory* 19.2 (2016), pp. 233–238. ISSN: 1433-5883. DOI: `10.1515/jgth-2015-0032`. URL: `https://doi.org/10.1515/jgth-2015-0032`.

[41] W. C. Waterhouse. *Introduction to affine group schemes.* Vol. 66. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1979, pp. xi+164. ISBN: 0-387-90421-2.

[42] A. J. Weir. “Sylow p-subgroups of the general linear group over finite fields of characteristic p”. In: *Proc. Amer. Math. Soc.* 6 (1955), pp. 454–464. ISSN: 0002-9939. DOI: `10.2307/2032788`. URL: `https://doi.org/10.2307/2032788`.

[43] J. S. Wilson. “Groups with every proper quotient finite”. In: *Proc. Cambridge Philos. Soc.* 69 (1971), pp. 373–391. ISSN: 0008-1981. DOI: `10.1017/s0305004100046818`. URL: `https://doi.org/10.1017/s0305004100046818`.

[44] J. S. Wilson. “Large hereditarily just infinite groups”. In: *J. Algebra* 324.2 (2010), pp. 248–255. ISSN: 0021-8693. DOI: `10.1016/j.jalgebra.2010.03.023`. URL: `https://doi.org/10.1016/j.jalgebra.2010.03.023`.

[45] I.O. York. “The group of formal power series under substitution.” PhD thesis. University of Nottingham, 1990.

Thanks to...

I am not used to include in my academic works an entire section just for thanking people. However, this thesis represents somehow a full stop for an incredible part of my life, for better or worse; thus I feel, in some sense, the necessity of thanking people that have been around me in the meanwhile.

In every PhD student's career — I think — sooner or later some down day arrives. Thus I start thanking the other PhD students and post-doc researchers, that I share most of my time at university with, and that allowed me to reply "the guys are very nice" to people asking how my work was going. In particular, I must thank Alice, Lorenzo and Mauro, that shared with me most of fears, anxieties, deadlines... as well as most of courses and mathematical experiences.

I'd also like to thank the "Düsseldorf crew". Besides prof. Benjamin Klopsch — that I have already mentioned in the acknowledgements — I'm debt to all young mathematicians that hosted me in their university (and sometimes in their office!) while I was there. Especially, I thank Matteo Vannacci and Ilir Snopce for the fruitful talks, either mathematical or not.

I thank my family, in particular my brother Giona that gave me also some technical suggestions for this thesis.

Finally, let me conclude switching to Italian.

Questa tesi è dedicata a Simone. Per tutto: per i giochi, per le vacanze insieme, le corse serali, le prese in giro, per i barometri ad acqua stesi per quattro piani, per i video assurdi, per aver cercato (inutilmente) di spiegarmi l'arte grafica e il funzionamento dei motori, per i mille progetti realizzati e i diecimila solo pensati (volentieri davanti a un alcolico). Per le imprese senza speranza, fallite già in partenza; per la SD-Omino, che sotto-sotto speravamo sarebbe davvero diventato il nostro lavoro, qualunque cosa fosse. Per esserci sempre stato, discretamente, più di quanto io non ci sia stato per lui. Perché è incredibile scoprire quanto possa mancare qualcuno che ti dica "Gaga, non fare la cacchetta!". Meriterebbe qualcosa di più di una dedica in una mediocre tesi di dottorato. Mi spiace, per intanto dovrà accontentarsi.

Ed è anche dedicata a Enea. Per tutti i suoi chili di tenerezza; per gli "aoo", gli "nghé" e per tutti gli altri versi poetici che hanno accompagnato la stesura di queste pagine. Per non aver eccessivamente boicottato la stessa (il giusto...). Per avermi regalato un'altra prospettiva sulla vita.

Questa tesi *non* è invece dedicata a Priscilla. A lei dovrebbe esserle dedicato ogni istante. Perché ogni giorno, sopporta (quasi ;-)) pazientemente il disordine e la distrazione e sprona un eterno indeciso. Perché mi è stata vicino e mi ha aiutato quando ce ne è stato bisogno. Forse su queste pagine c'è più di lei di quanto si possa immaginare.