Automorphisms of Local Fields and Zeta Functions of some Infinite Groups

Inaugural-Dissertation

zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Djurre Jacob Tijsma

aus Leeuwarden, die Niederlande

Düsseldorf, April 2022

aus dem Institut für Mathematik
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Berichterstatter:

1. Prof. Dr. Benjamin Klopsch
2. Prof. Dr. Britta Späth

Tag der mündlichen Prüfung: 27.06.2022

Abstract

This dissertation consists of three different research projects within group theory and it is written as a cumulative thesis.

The first project is about automorphisms of local fields and consists of the article [14]:

- With Jakub Byszewski and Gunther Cornelissen; *Automata and finite order elements in the Nottingham group*, J. Algebra **602** (2022), 484–554.

This article appears as a self-contained chapter in the thesis. The Nottingham group at a prime number p consists of power series $t+a_2t^2+a_3t^3+\cdots$ in the variable t with coefficients a_i from the field of p elements, where the group operation is given by composition of power series. Only a handful of power series of finite order are explicitly known through a formula for their coefficients. We argue in this article that it is advantageous to describe such series in closed computational form through automata. We give an explicit automaton-theoretic description of some series of order 4 and 8; and an embedding of the Klein four-group in the Nottingham group at 2. Moreover, we study the complexity of the new examples from the algebro-geometric properties of the equations they satisfy.

The second project concerns the commensurability zeta function, a recent type of zeta function for groups introduced in 2020 by Bou-Rabee and Studenmund. This zeta function was defined in analogy to the subgroup zeta function. Two subgroups of an ambient group are said to be commensurable, if their intersection has finite index in both groups. The product of these two numbers is the commensurability index. Fixing some subgroup of the ambient group, we consider all subgroups which are commensurable with this fixed subgroup and we encode the corresponding commensurability index in a Dirichlet series, the commensurability zeta function. We compute this zeta function for the free abelian groups of finite rank and show that it can be expressed as a quotient of zeta functions arising from counting subgroups of finite index. Moreover, we generalise the commensurability zeta function to the setting of modules.

The final project contains an investigation into the subject of normal subgroup growth. The normal subgroup zeta function of a group is a Dirichlet series encoding the number of normal subgroups of each finite index. By making use of an identity for Lie algebras of Chevalley type A_* we derive for a family of groups a general formula for the normal subgroup zeta function. Together with extensive Lie algebra calculations, we obtain general properties of the normal subgroup zeta function of $\mathrm{SL}_d^1(\mathcal{O})$ with $\mathcal{O}$ the ring of integers of a non-Archimedean local field. In some specific cases, i.e. $\mathrm{SL}_2^1(\mathbf{Z}_p)$, $\mathrm{SL}_3^1(\mathbf{Z}_p)$ and $\mathrm{SL}_3^1(\mathbf{F}_p[\![T]\!])$, we obtain an explicit formula for the normal subgroup zeta function.

Acknowledgements

First and foremost of all I would like to thank my supervisor Benjamin Klopsch for not only giving me the possibility for this work, but also for his support and guidance throughout my PhD. Further I wish to express my sincere thanks to my co-supervisor Britta Späth.

I am grateful to my collaborators Jakub Byszewski and Gunther Cornelissen for introducing me to the Nottingham group and for the fruitful and interesting collaboration. I would like to thank Ilir Snopce for suggesting the topic of normal subgroup zeta functions and providing me with initial input, based on rudimentary handwritten notes from discussions with Benjamin Klopsch.

I am thankful to Ragnar Groot Koerkamp for his collaboration for setting up a computer search for small automata. Finally, I would like to express my sincere thanks to Moritz Petschick for proofreading parts of my thesis.

The research was conducted in the framework of the research training group GRK 2240: *Algebro-Geometric Methods in Algebra, Arithmetic and Topology*, which is funded by the DFG to which I am greatful for the financial support I enjoyed.

Contents

Chapter 1

Introduction and general overview

This dissertation consists of three different research projects within group theory and it is written as a cumulative thesis. The first project is about automorphisms of local fields and consists of the article:

- With Jakub Byszewski and Gunther Cornelissen; *Automata and finite order elements in the Nottingham group*, J. of Algebra **602** (2022), 484–554.

The article appears as a self-contained chapter in the thesis. It is preceded by a two page summary of my contribution to this article during my time as a PhD student at the HHU Düsseldorf; see Chapter 3. The second and third project are both about zeta functions of infinite groups. The second project concerns the commensurability zeta function; see Chapter 4. The third project is about the normal subgroup zeta function; see Chapter 5. Chapter 4 and Chapter 5 both start with an introduction into the subject.

The three projects are preceded by the preliminary Chapter 2, where we introduce some basic notions which will be of use in the later chapters. The references for the introduction, Chapter 2, Chapter 4, Chapter 5 and the two page explanation of Chapter 3 are collected at the end. The paper in Chapter 3 has its own bibliography.

Automorphisms of local fields

All references to theorems, propositions, equations, figures and tables are to the paper *Automata and finite order elements of the Nottingham group* (see Chapter 3), all citations can be found in the bibliography at the end of this thesis.

In Chapter 3 we study finite order elements in the Nottingham group. In very elementary terms this comes down to the following. Suppose

$$\sigma(t) = t + a_2t^2 + a_3t^3 + a_4t^4 + \cdots \neq t \tag{1.1}$$

is a formal power series in the variable t with coefficients from the field $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ with two elements. Since $\sigma(t) = t + O(t^2)$, substituting $\sigma(t)$ into itself produces a power series

$$\sigma^{\circ 2}(t) = t + a_2(a_3 + 1)t^4 + \cdots ,$$

and one may iterate this process to arrive at $\sigma^{\circ N}(t) = \sigma(\sigma(\cdots\sigma(t)))$ (N-fold composition). We are interested in *the explicit description of* σ *and* N *for which* $\sigma^{\circ N}(t) = t$ (this is only possible if N is a power of 2). Our goal is not to compute finitely many coefficients a_i of such $\sigma(t)$, but rather to give a *finite description* of the complete series.

For a fixed prime number p, the *Nottingham group* $\mathcal{N}(\mathbf{F}_p)$ is the pro-p-Sylow subgroup of the group of ring automorphisms $\mathrm{Aut}(\mathbf{F}_p[\![t]\!])$ of the formal power series ring $\mathbf{F}_p[\![t]\!]$ over the finite field $\mathbf{F}_p$, with composition as multiplication. There is a group isomorphism $\mathrm{Aut}(\mathbf{F}_p[\![t]\!]) \cong \mathcal{N}(\mathbf{F}_p) \rtimes \mathbf{F}_p^*$. A ring endomorphism σ of $\mathbf{F}_p[\![t]\!]$ is determined uniquely by the image $\sigma(t) \in t\mathbf{F}_p[\![t]\!]$ of t, and $\mathcal{N}(\mathbf{F}_p)$ is identified with the group of power series $\sigma(t) \in \mathbf{F}_p[\![t]\!]$ with $\sigma(t) = t + O(t^2)$ under composition. The *depth* of $\sigma = \sigma(t) \in \mathcal{N}(\mathbf{F}_p)$ is $d(\sigma) = \mathrm{ord}_t(\sigma(t) - t) - 1$ (and $d(t) = \infty$), so if $\sigma(t) = t + a_kt^k + O(t^{k+1})$ with $a_k \neq 0$, then $d(\sigma) = k - 1$. The *lower break sequence* of an element $\sigma \in \mathcal{N}(\mathbf{F}_p)$ of finite order p^n is defined as $(d(\sigma^{\circ p^i}))_{i=0}^{n-1}$. The lower break sequence of $\sigma \in \mathcal{N}(\mathbf{F}_p)$ of order p^n is a refined invariant with the property that there are only finitely many conjugacy classes of elements of fixed order p^n with a given break sequence [41]. The method of Lubin [41] can in principle be used to count that number using results from local class field theory. In the same article there is an exact characterisation of the possible lower break sequences.

We can rephrase our goal now as follows: give a finite description of the complete series of finite order elements in $\mathcal{N}(\mathbf{F}_p)$.

The Nottingham group arises in many areas within mathematics.

- In *group theory*, every countably based pro-p group embeds into $\mathcal{N}(\mathbf{F}_p)$ Camina [15]; in particular every finite p-group embeds into $\mathcal{N}(\mathbf{F}_p)$ (an older unpublished result of Leedham-Green and Weiss; see [15, Thm. 3]).

- In *number theory* the Nottingham group occurs naturally in the theory of wild ramification (as the group of wild automorphisms of $\mathbf{F}_p((t))$; see Fesenko [25]).
- The previous point also relates to *algebraic geometry*. Namely: if a group G acts on a smooth projective curve X over $\mathbf{F}_p$, then the stabiliser G_x of a point $x \in X$ acts on the completion of the local ring $\mathcal{O}_{X,x}$. This completion is isomorphic to $\mathbf{F}_p[\![t]\!]$, leading to an embedding of the wild ramification group G_x^1 (the p-Sylow subgroup of G_x) into $\mathcal{N}(\mathbf{F}_p)$; one can, for example, study deformations of group actions on curves through deformations of this group homomorphism, much like deformations of linear group representations, e.g. of Galois groups, cf. [49].

Klopsch proved that every element of order p in $\mathcal{N}(\mathbf{F}_p)$ is conjugate to

$$t/\sqrt[m]{1 - mat^m} = t + at^{m+1} + \cdots \tag{1.2}$$

for some positive integer m coprime to p and $a \in \mathbf{F}_p^*$, and that these series are mutually not conjugate [35]. In [41, §4] Lubin gave another proof of this result by using local class field theory. The expression (1.2) may be readily converted into a formula for the coefficients of the corresponding power series by applying the binomial expansion.

Jean [32] and Lubin [41] indicated how to use formal groups and explicit local class field theory to describe elements of any order p^n in $\mathcal{N}(\mathbf{F}_p)$, and iterative procedures for the calculation of the coefficients of such elements were described (compare [31], [34], [6, §6]). However, the only known formulas for elements of order p^n for $n > 1$ are for $p^n = 4$ in $\mathcal{N}(\mathbf{F}_2)$, given by Jean in [31, Ch. 7], Chinburg and Symonds [16], and Scherr and Zieve (cf. [5, Rem. 1.4]). The Chinburg–Symonds example represents the action of an automorphism of order 4 on the local completed ring at zero of the supersingular elliptic curve over $\mathbf{F}_2$; compare also [5, Sect. 1], where it is argued that this is essentially the only example that can be constructed by such a method; more precisely, up to conjugation, it is the only 'almost rational' example.

A variety of techniques have been used so far in attempts to tackle the problem of describing the complete series of finite order elements in $\mathcal{N}(\mathbf{F}_p)$, with various degrees of success. We argue that it is advantageous to describe such series in closed computational form through automata. A *p-automaton* is a finite directed multigraph (allowing loops, as well as multiple edges between vertices) for which:

- vertices are labelled by elements of $\mathbf{F}_p$;
- one vertex (the so-called *start vertex*) is additionally marked 'Start';
- each vertex has exactly p outgoing edges, each labelled by a different element of the set $\{0, 1, \ldots, p-1\}$;

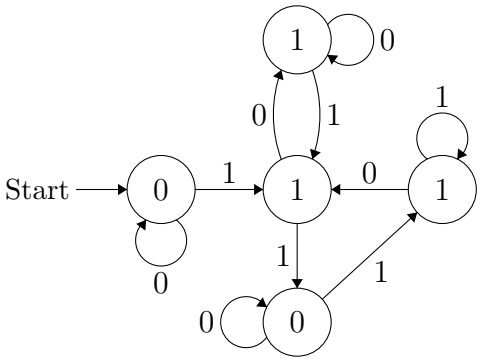


Figure 1.1: A 2-automaton representing the element $\sigma_{\min}$ of $\mathcal{N}(\mathbf{F}_2)$ of order 4 with lower break sequence $(1, 3)$.

- there is a path in the automaton from the start vertex to any vertex;
- an edge with label 0 always connects two (not necessarily different) vertices with the same label.

In the general theory of automata, this is called a 'leading zeros invariant p-DFAO (deterministic finite p-automaton with output) with output alphabet $\mathbf{F}_p$ and all states accessible' (vertices are also called 'states'); see [1, 4.3]. An example of such an automaton is given in the figure on this page.

A p-automaton produces a so-called *p-automatic sequence* $(a_k)_{k\geq 0}$, where a_k is the label carried by the final vertex of the walk that starts at the start vertex and follows the edges according to the successive digits of k in base p (starting from the least significant digit, also called the 'reverse/backwards reading convention', compare [1, 12.2]). The sequence $(a_k)_{k\geq 0}$ gives rise to the corresponding formal power series $\sum_{k=0}^{\infty} a_k t^k$ over $\mathbf{F}_p$ in the variable t. The fifth property of a p-automaton means that we can allow the base-p expansion of k to have any number of leading zeros without affecting the resulting sequence.

For example, the automaton in Figure 1.1 corresponds to the power series

$$\sigma_{\min}(t) = t + t^2 + t^4 + t^5 + O(t^6).$$

To illustrate our reading conventions, we compute the coefficient of t^{13} in the series $\sigma_{\min}$: write $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ in base 2 as 1101; begin at the start vertex and follow the directed edges with respective labels $1, 0, 1, 1$; we end up in a vertex with label 0, so $a_{13} = 0$.

The construction of elements of order p^n in $\mathcal{N}(\mathbf{F}_p)$ starts with constructing a cyclic Galois extension of order p^n of the field $\mathbf{F}_p(\!(z)\!)$ of Laurent series through the use of Witt

vectors [40, p. 107, Thm. 5]. This gives us explicit generators α_i, satisfying algebraic relations over $\mathbf{F}_p(\!(z)\!)$, for the field extension and we get an explicit formula for the action of a generator σ of the Galois group. By choosing a uniformiser t, given as a rational function in the α_i, for this extension, we get an explicit expression for $\sigma(t)$ as a rational function of the α_i. With the help of a Groebner basis algorithm we can eliminate the variables α_i, giving an explicit equation $F(t, X) = 0$ for $\sigma = \sigma(t)$ over the field $\mathbf{F}_p(t)$. We can always reduce to the case where $F(t, X)$ is irreducible, in which case it is shown in Proposition 9.2.1 that $\deg_t F = \deg_X F$. Since σ is an automorphism of $\mathbf{F}_p(\!(t)\!)$, we have found an algebraic equation over $\mathbf{F}_p(t)$ satisfied by the element $\sigma(t)$ in $\mathcal{N}(\mathbf{F}_p)$ of order p^n.

This explicit equation $F(t, X) = 0$ allows us to pass to the realm of automata using Christol's theorem. Christol's theorem says that a power series $\sigma = \sum_{k=0}^{\infty} a_k t^k \in \mathbf{F}_p[\![t]\!]$ is algebraic over $\mathbf{F}_p(t)$ if and only if the sequence $(a_k)_{k\geq 0}$ is p-automatic [19, 20]. Hence we have a theoretical method for constructing automata corresponding to elements of $\mathcal{N}(\mathbf{F}_p)$ of order p^n for any positive integer n. Once the equation has been fixed the construction of the automata has been automated. Three methods for constructing automata starting with an equation are discussed in Section 3, they are based upon spaces of differential forms [10], equations in Ore form [20, 53] and diagonals of two variable power series [53]. The size of the resulting automaton depends heavily on the choice of extension $\mathbf{F}_p(\!(z)\!)$ and the chosen uniformiser t. Within a conjugacy class of an element of order p^n in $\mathcal{N}(\mathbf{F}_p)$ the minimal size of an automaton representing a power series can vary greatly.

Our method is valid for every prime number, but we limit ourselves here to the case $p = 2$. For primes $p > 2$ the automata we computed tended to be so large (e.g. an order 9 automaton with 3634 states), that they were difficult to study, whereas for $p = 2$ we found many small and managable automata. The next theorem describes elements of order 4 in $\mathcal{N}(\mathbf{F}_2)$ with a 'small' break sequence up to conjugation in $\mathcal{N}(\mathbf{F}_2)$ in terms of automata.

Theorem 1.0.1 (Cor. 3.1.2 & Props. 3.4.1, 4.2.1, 5.2.1, 5.3.1)**.** *The following is a complete list representing all possible elements of order* 4 *in* $\mathcal{N}(\mathbf{F}_2)$ *with break sequence* $(1, m)$ *for all admissible values* $m < 10$*, up to conjugation in* $\mathcal{N}(\mathbf{F}_2)$:

- *with break sequence* $(1, 3)$: *two (previously known) series* σ_{CS} *and* $\sigma_{\mathrm{CS}}^{\circ 3}$ *given in Equations* (12) *and* (13)*, with the corresponding automata displayed in Table* 1*. The series* σ_{CS} *is conjugate in* $\mathcal{N}(\mathbf{F}_2)$ *to a new series* $\sigma_{\min}$ *described by the automaton in Figure* 2*, which is the unique series of order* 4 *described by a* 2*-automaton with at most* 5 *states.*
- *with break sequence* $(1, 5)$: *a series* $\sigma_{(1,5)}$ *corresponding to the* 13*-state automaton displayed in Figure* 5*.*
- *with break sequence* $(1, 9)$: *a series* $\sigma_{(1,9)}$ *with* 110*-state automaton described in Table* 2*.*

In Section 4 we present an algorithm for finding, for fixed integers N and n, all minimal 2-automata representing an element of finite order 2^n in $\mathcal{N}(\mathbf{F}_2)$ with at most N states [26]. For some of the automata it is possible to extract a manageable *closed formula* for the power series. We present five new such formulas for power series of order 4: $\sigma_{\mathrm{J}}^{\circ 3}$ displayed in Equations (16) & (17) and $\sigma_{\mathrm{T},1}, \sigma_{\mathrm{T},2}, \sigma_{\mathrm{T},3}$ and $\sigma_{\mathrm{T},4}$ in Table 3. In the literature there are no known explicit descriptions of the complete series of finite order $p^n > 4$ in $\mathcal{N}(\mathbf{F}_p)$. The next theorem gives the first descriptions of the complete series of order 8 elements in terms of automata.

Theorem 1.0.2 (Props. 7.1.1, 7.2.1 & 7.3.1)**.** *Up to conjugation in $\mathcal{N}(\mathbf{F}_2)$, there are precisely* 4 *elements $\sigma_8, \sigma_8^{\circ 3}, \sigma_{8,2}, \sigma_{8,2}^{\circ 3}$ of order* 8 *with 'minimal' break sequence* $(1, 3, 11)$ *in $\mathcal{N}(\mathbf{F}_2)$, where σ_8 corresponds to the* 320*-state automaton given in Table* 7.2 *, and $\sigma_{8,2}$ corresponds to the* 926*-state automaton described in* 7.3*.*

Every finite 2-group embeds in $\mathcal{N}(\mathbf{F}_2)$, so one might wonder if it is possible to give a description in terms of automata for non-cyclic subgroups of $\mathcal{N}(\mathbf{F}_2)$. The next theorem affirms this for the Klein four-group; see Section 8.3 for more on non-cyclic subgroups of $\mathcal{N}(\mathbf{F}_2)$.

Theorem 1.0.3 (Props. 8.1.2 & 8.2.1)**.** *For every embedding of the Klein four-group V in the Nottingham group $\mathcal{N}(\mathbf{F}_2)$, some nontrivial element of V has depth at least* 5*. Furthermore, the series $\sigma_{V,1}$ and $\sigma_{V,2}$ corresponding to the automata depicted in Table* 6 *have break sequences* (1) *and* (5) *and exhibit an explicit embedding of two generators of the Klein four-group into $\mathcal{N}(\mathbf{F}_2)$.*

To try to quantify our goal of giving finite descriptions of the complete series of finite order elements in $\mathcal{N}(\mathbf{F}_2)$ we studied the notion of *sparseness* in relation to our finite order series. A series $\sum_{k=0}^{\infty} a_k t^k \in \mathbf{F}_2[\![t]\!]$ is called *sparse* if the number of non-zero coefficients up to N grows like $\log(N)^r$ for some real $r \geq 0$. Cobham showed in [17] a dichotomy for series in $\mathcal{N}(\mathbf{F}_2)$: either a series is sparse or the number of non-zero coefficients up to N grows like N^α for some real $\alpha > 0$. We write S for the set of all sparse series in $\mathcal{N}(\mathbf{F}_2)$ and $\widehat{S}$ for the series in $\mathcal{N}(F_2)$ which are sparse up to multiplication by an element of $\mathbf{F}_2(t)$. We also introduce a third set $\hat{\hat{S}}$, which we do not define here. In Theorem 11.2.6 we discuss which of the series in the article belong to $S, \widehat{S}$ or $\hat{\hat{S}}$. In some cases, see Proposition 12.2.1, the automaton of $\sigma \in \mathcal{N}(\mathbf{F}_2)$ can be used to decide if $\sigma \notin \widehat{S}$.

Our investigation of finite order elements in $\mathcal{N}(\mathbf{F}_p)$ through the use of automata has provided us with many more interesting questions. It would be interesting to have examples of finite order elements in $\mathcal{N}(\mathbf{F}_p)$ with order $p^n > 4$ that have small automata. In Theorem 1.0.3 we gave an example of an embedding of a non-cyclic group in $\mathcal{N}(\mathbf{F}_2)$ with break sequences $(1), (1), (5)$. What are the possible break sequences for embeddings of the Klein four-group in $\mathcal{N}(\mathbf{F}_2)$, and more generally for arbitrary p-groups into $\mathcal{N}(\mathbf{F}_p)$. We

looked at embeddings of finite groups into $\mathcal{N}(\mathbf{F}_p)$, a challenge would be to study embeddings of infinite groups in $\mathcal{N}(\mathbf{F}_p)$ through automata. For example the free group on two generators or the Grigorchuk group. An interesting question related to sparseness is, if every conjugacy class of a finite order element in $\mathcal{N}(\mathbf{F}_p)$ contains a sparse representative.

Zeta functions of some infinite groups

Commensurability zeta function

In Chapter 4 we study the commensurability zeta function. Let G be a group and let $H, K \leq G$ be two subgroups of G. We say that the groups H and K are *commensurable* (in the strict sense as subgroups of G), if their *commensurability index*

$$c(H,K) = |H : H \cap K| \cdot |K : H \cap K|$$

is finite. This is a generalisation of the notion of commensurability for real numbers, two non-zero real numbers are said to be commensurable if their ratio is a rational number. Clearly, every two subgroups of a finite group are commensurable. Examples of two non-commensurable subgroups of a group are also easy to be found. For example, take any infinite group and consider two subgroups, one which is finite and one that is infinite. Fixing a subgroup $K \leq G$, we consider the *commensurability function*

$$c^{G,K} : \mathbf{N} \to \mathbf{N} \cup \{0, \infty\}, \quad n \mapsto c_n^{G,K},$$

where

$$c_n^{G,K} = |\{H \leq G \mid c(H,K) = n\}|,$$

i.e. the number of subgroups of G having commensurability index n with K. In case the commensurability function $c^{G,K} : \mathbf{N} \to \mathbf{N} \cup \{0, \infty\}$ takes on only finite values, we associate to the pair (G, K) the *commensurability zeta function for the pair* (G, K), denoted by $\zeta_{G,K}^{\mathrm{comm}}(s)$, which is the (formal) Dirichlet series

$$\zeta_{G,K}^{\mathrm{comm}}(s) = \sum_{n=1}^{\infty} c_n^{G,K} n^{-s}, \quad s \in \mathbf{C}.$$

The abscissa of convergence of the zeta function $\zeta_{G,K}^{\mathrm{comm}}(s)$ is related to the growth type of the *commensurability growth function* $s^{G,K}$, which is defined by

$$s^{G,K} : \mathbf{N} \to \mathbf{N}, \quad n \mapsto s_n^{G,K} = \sum_{k=1}^{n} c_k^{G,K}.$$

In the following we study properties of the commensurability zeta function, for instance how the algebraic properties of the groups G, K control the analytic properties of $\zeta_{G,K}^{\mathrm{comm}}(s)$

and vice versa. This is similar to other zeta functions counting other substructures such as the (normal, subnormal, maximal) finite-index subgroups or the finite dimensional representations over $\mathbf{C}$; for some examples see [27, 63]. We do have an additional flexibility, since we consider a pair (G, K) of groups instead of a single group G.

In [8] the commensurability function is studied for the class of unipotent algebraic $\mathbf{Z}$-groups; e.g. algebraic group defined over $\mathbf{Z}$, see also [52]. For every unipotent algebraic $\mathbf{Z}$-group G Bou-Rabee and Studenmund prove that the commensurability function of its real Lie group $G(\mathbf{R})$, with respect to the arithmetic lattice $G(\mathbf{Z})$, takes only finite values. Therefore the corresponding commensurability zeta function of the pair $(G(\mathbf{R}), G(\mathbf{Z}))$ is defined. They show that the zeta function $\zeta^{\mathrm{comm}}_{G(\mathbf{R}),G(\mathbf{Z})}(s)$ admits the formal Euler product

$$\zeta^{\mathrm{comm}}_{G(\mathbf{R}),G(\mathbf{Z})}(s) = \prod_p \zeta^{\mathrm{comm},p}_{G(\mathbf{R}),G(\mathbf{Z})}(s),$$

where p runs over all prime numbers and where the functions

$$\zeta^{\mathrm{comm},p}_{G(\mathbf{R}),G(\mathbf{Z})}(s) = \sum_{n=0}^{\infty} c_{p^n}^{G(\mathbf{R}),G(\mathbf{Z})} p^{-ns}$$

are called the local factors. The local factors enumerate the subgroups of G whose commensurability index with K is a power of the prime number p. Using techniques from model theory and p-adic integration [46], previously succesfully applied to the area of subgroup growth (see [45, Chapter 15 and Window 12]), they prove that the local factors $\zeta^{\mathrm{comm},p}_{G(\mathbf{R}),G(\mathbf{Z})}(s)$ are rational functions over $\mathbf{Q}$ in p^{-s}. Moreover, there are bounds on the degree of the numerator and denominator of these rational functions, that are independent of the prime number p. This mirrors a similar behaviour of the zeta functions related to subgroup growth and representation growth; see [27, 30].

The only example, of an explicitly computed commensurability zeta function for a pair of different groups, known to Bou-Rabee and Studenmund, is the commensurability zeta function for the pair $(\mathbf{R}, \mathbf{Z})$ of abelian groups [8, Prop. 2.1], which they compute as

$$\zeta^{\mathrm{comm}}_{\mathbf{R},\mathbf{Z}}(s) = \frac{\zeta(s)^2}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s},$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the ordinary Riemann zeta function and $\omega(n)$ counts the number of different prime factors of n. Any subgroup of $\mathbf{R}$, which is commensurable with $\mathbf{Z}$, is actually a subgroup of $\mathbf{Q}$, so in fact $\zeta^{\mathrm{comm}}_{\mathbf{R},\mathbf{Z}}(s) = \zeta^{\mathrm{comm}}_{\mathbf{Q},\mathbf{Z}}(s)$. In [9] Bou-Rabee, Kaletha and Studenmund compute some asymptotics of the commensurability growth function $s^{G,\Gamma}$ for a Chevalley group scheme G defined over $\mathbf{Z}$ of rank greater than 1 and an arithmetic lattice Γ in $G(\mathbf{R})$. They show that the asymptotic behaviour of $s^{G,\Gamma}$ depends on the subgroup growth function $n \mapsto \sum_{k=1}^{n} a_k(\Gamma)$ of Γ and a constant depending only on the root system of G.

Our contribution to the study of the commensurability function is the explicit computation of the commensurability zeta functions for an infinite family of pairs of groups. This extends the current list of known examples from a single one to infinitely many. Not only does this give more examples to test hypotheses on, it also shows an interesting and unexpected connection to the theory of subgroup growth, as we can express the commensurability zeta function completely in terms of a subgroup zeta function.
We compute for any positive integer $d \in \mathbf{N}$ for the pair $(\mathbf{R}^d, \mathbf{Z}^d)$ of abelian groups the commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{R}^d,\mathbf{Z}^d}(s) = \zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$; see Theorem 1.0.4. In the wording of [8] this covers the case where G is an abelian unipotent connected algebraic group defined over $\mathbf{Z}$. Because G is defined over $\mathbf{Z}$, G is $\mathbf{Q}$-isomorphic to a $\mathbf{Q}$-vector group H (see [33, Appendix A.3]), so that $G(\mathbf{R}) \cong H(\mathbf{R}) \cong \mathbf{R}^d$ for some $d \in \mathbf{N}$. Under this $\mathbf{Q}$-isomorphism the image of $G(\mathbf{Z})$ is commensurable with $H(\mathbf{Z})$ [52, Prop. 4.1], which is a lattice of full rank in $H(\mathbf{R})$. Any two lattices of full rank inside $\mathbf{R}^d$ have the same commensurability zeta function and since any lattice of full rank in $\mathbf{R}^d$ which is commensurable with $\mathbf{Z}^d$ lies in $\mathbf{Q}^d$, we can reduce our computation to the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ of abelian groups.

The next theorem shows that the commensurability zeta function for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ is related to the subgroup zeta function of $\mathbf{Z}^d$. Actually, this theorem is obtained as a corollary of a more general statement, see Theorem 4.1.5, which deals with a generalisation of the commensurability function of pairs of abelian groups to modules.

Theorem 1.0.4. *Let $d > 0$ be an integer. The commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ of abelian groups satisfies*

$$\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s) \cdot \zeta^{\leq}_{\mathbf{Z}^d}(2s) = \zeta^{\leq}_{\mathbf{Z}^d}(s)^2, \tag{1.3}$$

where $\zeta^{\leq}_{\mathbf{Z}^d}(s)$ denotes the subgroup zeta function of $\mathbf{Z}^d$.

The proof of Theorem 1.0.4 not only shows that the commensurability zeta function satisfies equation (1.3), but actually explains the connection between the commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ and the subgroup zeta function $\zeta^{\leq}_{\mathbf{Z}^d}(s)$. Therefore the equation (1.3) is more than a coincidence of Dirichlet series. Two alternative proofs for Theorem 1.0.4 are given in the appendix for the cases $d \in \{2, 3\}$; one proof uses a standard basis for lattices and the other proof uses the Bruhat-Tits building. It is a well-known result, see [45, Chapter 15] for multiple proofs, that the subgroup zeta function for $\mathbf{Z}^d$ is given by

$$\zeta^{\leq}_{\mathbf{Z}^d}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1),$$

where $\zeta(s)$ is the ordinary Riemann zeta function. Consequently, by using Theorem 2.0.3, we have the following corollary of Theorem 1.0.4, describing the commensurability growth.

Corollary 1.0.5. *Let $d > 0$ be an integer. The commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ is given by the formula*

$$\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s) = \prod_{k=0}^{d-1} \frac{\zeta(s-k)^2}{\zeta(2s-k)}$$

and hence the commensurability growth $n \mapsto s_n^{\mathbf{Q}^d,\mathbf{Z}^d}$ *of the pair* $(\mathbf{Q}^d, \mathbf{Z}^d)$ *satisfies*

$$s_n^{\mathbf{Q}^d,\mathbf{Z}^d} \sim \frac{C}{d} n^d \log(n) \quad as \quad n \to \infty,$$

where the constant C *is given by*

$$C = \frac{\zeta(2)^2 \zeta(3)^2 \cdots \zeta(d)^2}{\zeta(d+1)\zeta(d+2)\cdots\zeta(2d)}.$$

We prove Theorem 1.0.4 not directly. Instead, we formulate the concept of the commensurability function for modules and then prove a general theorem for a specific class of modules; see Theorem 4.1.5. Theorem 1.0.4 is then obtained as a corollary of Theorem 4.1.5.

Normal subgroup zeta function

In Chapter 5 we study the normal subgroup zeta function of a specific family of groups. Let G be a group. Define for every positive integer $n \in \mathbf{N}$ the number $a_n^{\trianglelefteq}(G)$ by

$$a_n^{\trianglelefteq}(G) = |\{H \trianglelefteq G \mid |G : H| = n\}|,$$

i.e. the number of normal subgroups of G of index n. In case the number $a_n^{\trianglelefteq}(G)$ is finite for every $n \in \mathbf{N}$, we define the *normal subgroup growth* of the group G by

$$s^{\trianglelefteq}(G) : \mathbf{N} \to \mathbf{N}, \quad m \mapsto s_m^{\trianglelefteq}(G) = \sum_{n=1}^{m} a_n^{\trianglelefteq}(G),$$

i.e. $s_m^{\trianglelefteq}(G)$ equals the number of normal subgroups of G of index at most m, and we define the corresponding *normal subgroup zeta function*, or in short *normal zeta function*, of G by the (formal) Dirichlet series

$$\zeta_G^{\trianglelefteq}(s) = \sum_{n=1}^{\infty} a_n^{\trianglelefteq}(G) n^{-s}, \quad s \in \mathbf{C}.$$

For a prime number p we write

$$\zeta_{G,p}^{\trianglelefteq}(s) = \sum_{n=0}^{\infty} a_{p^n}^{\trianglelefteq}(G) p^{-ns}, \quad s \in \mathbf{C},$$

for the *local factor* of $\zeta_G^{\trianglelefteq}(s)$ at p. When G is a profinite group, we should take into account the topology of G and we define $a_n^{\trianglelefteq}(G)$ to be the number of closed subgroups of G of index

n. In case G is a finitely generated profinite group, then a deep result by Nikolov and Segal, see [50], says that any abstract normal subgroup of G of finite index is open. So for these groups we do not need to incorporate the condition of being closed. Groups for which the numbers $a_n^{\trianglelefteq}(G)$ are finite for all $n \in \mathbf{N}$ are, for example, finitely generated groups, because these groups have finitely many subgroups of every finite index. Many interesting groups are finitely generated. When G is a profinite group and topologically finitely generated an analogous statement holds for closed subgroups of G.

In their seminal 1998 paper [27] Grunewald, Segal and Smith introduce, among other types of zeta functions of groups, the normal subgroup zeta function. For torsion-free finitely generated nilpotent groups G they show the existence of an Euler product

$$\zeta_G^{\trianglelefteq}(s) = \prod_p \zeta_{G,p}^{\trianglelefteq}(s),$$

where the product runs over all prime numbers p, rationality of the local factors $\zeta_{G,p}^{\trianglelefteq}(s)$ and more. They are interested in what the growth of the function $s^{\trianglelefteq}(G)$ can say about the algebraic properties of the group G and vice versa. For the closely related area of subgroup growth a clear answer is given for groups of polynomial subgroup growth, which were characterised as the virtually soluble groups of finite rank in 1993 by Lubotzky, Mann and Segal [42]. This is one of the greatest achievemenst of the area of subgroup growth. For normal subgroup growth there is no such result. It is remarked in the introduction of the article [4] by Barnea and Schlage-Puchta that a slight variation of [45, Prop. 1.3.2 (ii)] yields for groups $H \leq G$ with $|G : H| < \infty$ that $s_n^{\trianglelefteq}(G) \leq s_n^{\trianglelefteq}(H) n^{|G:H|}$ for all $n \in \mathbf{N}$. And so the difficult problem remains, if a finite index subgroup of a group G can have substantially more normal subgroups than the group G itself. In contrast to subgroup growth there are simply too many groups with polynomial normal subgroup growth (including, for instance, finitely generated infinite simple groups); even if one restricts to residually finite groups, which seems reasonable, it seems daunting to extract much useful information solely from the condition of polynomial normal subgroup growth. Typically it is difficult to compute explicitly the normal zeta functions of groups, even for nicely behaved families of groups such as compact p-adic analytic groups. Very little is known about the asymptotic behaviour of $s^{\trianglelefteq}(G)$ or the properties of the zeta function $\zeta_G^{\trianglelefteq}(s)$.

In the 2001 article [44] Lubotzky shows for any finitely generated group G and every $n \in \mathbf{N}$ that $s_n^{\trianglelefteq}(G) \leq n^{c\Omega(n)}$, with $c > 0$ some constant and where $\Omega(n)$ denotes the number of prime divisors of n with multiplicity. A result of Mann [47] shows that for a non-abelian free group G we have $s_n^{\trianglelefteq}(G) > n^{c \log(n)}$ for some $c > 0$ and infinitely many $n \in \mathbf{N}$. This shows that the normal subgroup growth type of non-abelian free groups is $n^{\log(n)}$; see [4] for the definition of the *type* of a function.

For free abelian groups the corresponding normal subgroup zeta function, which coincides with the subgroup zeta function, are well-known. For an integer $d > 0$ the normal

zeta function of the free abelian group $G = \mathbf{Z}^d$ of rank d is given by

$$\zeta^{\triangleleft}_{\mathbf{Z}^d}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1),$$

with $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ the ordinary Riemann zeta function, see [12, §1] or [45, Ch. 15] for five different proofs of this identity. Using the analytic properties of $\zeta^{\triangleleft}_{\mathbf{Z}^d}(s)$ it is possible to deduce the rate of growth of $s^{\triangleleft}_N(\mathbf{Z}^d)$ as a function of N. For torsion-free finitely generated nilpotent groups G many local factors of $\zeta^{\triangleleft}_G(s)$ are computed in [27]. In [62] Voll computes the normal zeta function of torsion-free finitely generated nilpotent groups of class 2 with small centres. This applies in particular to the Heisenberg group $H(R)$, which is for a ring R (commutative with 1) defined as the subgroup

$$H(R) = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} | a, b, c \in R \right\}$$

of $\mathrm{GL}_3(R)$. Specifically we have $\zeta^{\triangleleft}_{H(\mathbf{Z})}(s) = \zeta(s)\zeta(s-1)\zeta(3s-2)$. An important step in [62] is the use of the Mal'cev correspondence, which associates to a torsion-free finitely generated nilpotent group G a $\mathbf{Q}$-Lie algebra $\mathfrak{L}(G)$. In the case where G is of nilpotency class 2, we have for every prime number p that $\zeta^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{\mathfrak{L}(G),p}(s)$, with $\zeta^{\triangleleft}_{\mathfrak{L}(G),p}(s)$ enumerating the ideals of $\mathfrak{L}(G)$ of p-th power index. The local factors $\zeta^{\triangleleft}_{H(\mathcal{O}),p}(s)$ of the normal zeta function $\zeta^{\triangleleft}_{H(\mathcal{O})}(s)$, with $\mathcal{O}$ the ring of integers of a number field, have also recieved some considerable amount of attention. In [54, 55] the local factors $\zeta^{\triangleleft}_{H(\mathcal{O}),p}(s)$ have been computed for primes p which are unramified or non-split in $\mathcal{O}$; see also [22, Sect. 2] for further examples.

In general the computation of the normal zeta function of a group G is hard. However, sometimes we understand the structure of the group G well enough that we are able to compute the normal zeta function explicitly. In Chapter 5 we focus on a particular family of groups for which we can say something concrete about the normal zeta function and in some cases calculate the normal zeta function explicitly.

For the remainder of the introduction let K be a non-Archimedean local field, write $\mathcal{O}$ for the ring of integers of K, let $\mathfrak{p}$ be the unique maximal ideal of $\mathcal{O}$ and let $k = \mathcal{O}/\mathfrak{p}$ be the finite residue field of characteristic $\mathrm{char}\, k = p$. These local fields play a central role in algebraic number theory; typical examples are the field $\mathbf{Q}_p$ of p-adic numbers and the field $\mathbf{F}_p(\!(T)\!)$ of Laurent series over a finite field $\mathbf{F}_p$. Let $d > 1$ be an integer and consider the group $G_0 = \mathrm{SL}_d(\mathcal{O})$. For a positive integer $n \in \mathbf{N}$ the *n-th principal congruence subgroup* $G_n = \mathrm{SL}^n_d(\mathcal{O})$ of the group $G_0 = \mathrm{SL}_d(\mathcal{O})$ is defined by

$$\mathrm{SL}^n_d(\mathcal{O}) = \ker(\mathrm{SL}_d(\mathcal{O}) \to \mathrm{SL}_d(\mathcal{O}/\mathfrak{p}^n)),$$

here we consider the reduction of the matrix entries modulo $\mathfrak{p}^n$. The groups $\mathrm{SL}^n_d(\mathcal{O})$ are examples of pro-p groups.

In case K is the field $\mathbf{Q}_p$ of p-adic rational numbers or the field $\mathbf{F}_p((T))$ of Laurent series in T with coefficients in the finite field $\mathbf{F}_p$, the (normal) subgroup zeta functions of the groups $\mathrm{SL}_d^1(\mathcal{O})$ have been studied. In [45, Sect. 4.3] bounds for the subgroup growth of the groups $\mathrm{SL}_d^1(\mathcal{O})$ with $\mathcal{O} = \mathbf{F}_p[\![T]\!]$ are obtained. In some cases the normal subgroup zeta functions of the groups $\mathrm{SL}_d^1(\mathcal{O})$ have also been studied. In [58] Snopce computes the normal zeta function for the group $\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])$ for all prime numbers $p > 2$, showing that

$$\zeta^{\trianglelefteq}_{\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])}(s) = \frac{1 + (p^2+p+1)(t+t^2+pt^3)}{1-t^3}, \quad t = p^{-s},$$

from which it follows for an integer $m \in \mathbf{N}$ that

$$a^{\trianglelefteq}_{p^m}(\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])) = \begin{cases} p^2+p+1 & \text{if } 3 \nmid m \\ p^3+p^2+p+1 & \text{if } 3 \mid m. \end{cases}$$

For a fixed prime number $p > 2$ Snopce also shows that the group $\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])$ has the same normal zeta function as the group $\mathcal{Q}(s,r)$, defined by Ershov in [24]. In [21, Cor. 4.10] du Sautoy provides a formula for the normal zeta function of the groups $\mathrm{SL}_2^n(\mathbf{Z}_p)$ for $n \in \mathbf{N}$ and $p > 2$ a prime number. In Theorem 1.0.10 we compute the normal zeta function of $\mathrm{SL}_2^1(\mathbf{Z}_p)$ for prime numbers $p > 2$, which is different from the one presented in [21, Cor. 4.10]. We believe our formula is correct. We are supported in this by the paper [3] by Barnea and Guralnick, they prove in [3, Thm. 1.3] that the sequence $(a_n^{\trianglelefteq}(\mathrm{SL}_2^1(\mathbf{Z}_p)))_{n\geq 1}$ is eventually periodic. Whereas the formula in [21, Cor. 4.10] suggests that $a_n^{\trianglelefteq}(\mathrm{SL}_2^1(\mathbf{Z}_p))$ grows polynomially with n. It was pointed out by Klopsch in [36, p. 57], that there is a mistake in [21, Lem. 4.6]. This could possibly explain the different formula in [21, Cor. 4.10]. It is also worth mentioning that [3, Thm. 1.4] proves that $a_n^{\trianglelefteq}(\mathrm{SL}_d^1(\mathbf{F}_p[\![T]\!]))$ is not bounded as a function of n in case $p \mid d$ in contrast to the case $p \nmid d$, where it is bounded.

Our investigation into the normal zeta function of the groups $\mathrm{SL}_d^1(\mathcal{O})$ is motivated by a yet to be published paper titled *Normal subgroups of Chevalley groups* by Klopsch and Snopce [37]; generalising earlier work of Barnea, Guralnick and Snopce [3, 58]. They set out to prove the following. Let $\mathfrak{g}$ be a Chevalley Lie algebra over a field F, associated to a root system of Chevalley type X. Suppose that char $F \neq 2$, if X is one of A_*, B_*, C_*, D_*, F_4, and that char $F \neq 3$, if X is G_2. Let z be a non-central element of $\mathfrak{g}$, then $[\mathfrak{g}, [\mathfrak{g}, [\mathfrak{g}, x]]]$ equals $\mathfrak{g}$. In Theorem 1.0.6 we strengthen their result for the simple Lie algebras of Chevalley type A_*. The finiteness result discovered and proved by Klopsch and Snopce is very surprising. Besides its fundamental nature it has very tangible applications, as noted by Klopsch and Snopce. For instance, their result places severe restrictions on the normal subgroup structure and describe properties of the normal subgroup zeta functions of the groups $\mathrm{SL}_d^1(\mathcal{O})$ of increasing rank. In small cases, one should be able to compute the corresponding normal zeta functions explicitly. This is also what we do in Chapter 5.

For an overview of our method of computation see the introduction of Chapter 5. We translate the problem of counting the number of normal subgroups of $G = \mathrm{SL}_d^1(\mathcal{O})$ to

a problem solely about Lie algebras. Once we are working with Lie algebras, the next theorem is crucial. Write $\mathfrak{sl}_d(k)$ for the special linear Lie algebra of Chevalley type A_{d-1} over the field k with the usual bracket $[x, y] = xy - yx$ for $x, y \in \mathfrak{sl}_d(k)$; see Section 5.4.1. For a subspace $V \subseteq \mathfrak{sl}_d(k)$ we write $[\mathfrak{sl}_d(k), V]$ for the subspace of $\mathfrak{sl}_d(k)$ spanned by all the commutators $[x, y]$ with $x \in \mathfrak{sl}_d(k)$ and $y \in V$. Our next theorem extends earlier unpublished results for simple Lie algebras of Chevalley type A_*, as discussed in [37].

Theorem 1.0.6. *Let $d > 1$ be an integer and let k be a field with* $\operatorname{char} k \nmid 2d$. *For all non-zero $x \in \mathfrak{sl}_d(k)$ we have*

$$[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), x]] = \mathfrak{sl}_d(k).$$

Actually, a slightly stronger result is proven in Theorem 5.6.5 in Section 5.6.1, however the above theorem is all we need for our discussion. A consequence of the above theorem is Proposition 5.3.7. It states that any closed normal subgroup $\{1\} \neq N \trianglelefteqslant G$ satisfies

$$G_{n+2} < N \leq G_n, \quad N \not\subseteq G_{n+1}$$

for some $n \in \mathbf{N}$, here $G_n = \mathrm{SL}_d^n(\mathcal{O})$. Ultimately this leads to the next theorem, which presents a general formula for the normal zeta function of the groups $\mathrm{SL}_d^1(\mathcal{O})$. We prove this theorem in Theorem 5.3.14. For convenience we define the number $\delta_K \in \{0, 1\}$ by

$$\delta_K = \begin{cases} 1 & \text{when } K \text{ is an unramified extension of } \mathbf{Q}_p; \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 1.0.7 (Klopsch, Snopce, T.)**.** *Let $d > 1$ be an integer and let p be a prime number with $p \nmid 2d$. Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and residue class field k. Write $L = \mathfrak{sl}_d(k)$. The normal zeta function $\zeta_G^{\trianglelefteqslant}(s)$ for the group $G = \mathrm{SL}_d^1(\mathcal{O})$ is given by*

$$\zeta_G^{\trianglelefteqslant}(s) = \frac{1}{1 - |L|^{-s}} \sum_{0 \neq V \subseteq L} |L : V|^{-s} \left(\sum_{\delta_K V + [V,L] \subseteq W \subseteq L} |L : W|^{-s + \dim_{\mathbf{F}_p} V} \right),$$

where V, W are $\mathbf{F}_p$-subspaces of L.

The above expression shows that the normal zeta function of $\mathrm{SL}_d^1(\mathcal{O})$ is a rational function in p^{-s} and we also recover that the sequence $(a_n^{\trianglelefteqslant}(\mathrm{SL}_d^1(\mathcal{O})))_{n \geq 1}$ is eventually periodic; this generalises the result in [3, Thm. 1.3]. We see that the formula for the normal zeta function depends on the residue field k, but except for the occurrence of δ_K, it does not depend on the ramification behaviour of the maximal ideal $\mathfrak{p}$. We list two important corollaries.

Corollary 1.0.8 (Klopsch, Snopce, T.). *Let $d > 1$ be an integer, let p be a prime number with $p \nmid 2d$ and write $f = [k : \mathbf{F}_p]$ for the degree of the field extension $k/\mathbf{F}_p$. Then there exists a polynomial $Q(X, Y) \in \mathbf{Z}[X, Y]$ with $\deg_Y Q = 2(d^2 - d)f - 1$ such that*

$$\zeta^{\triangleleft}_{\mathrm{SL}^1_d(\mathcal{O})}(s) = \frac{Q(p, p^{-s})}{1 - (p^{-s})^{(d^2-1)f}}.$$

Corollary 1.0.9. *Let $d > 1$ be an integer and let p be a prime number with $p \nmid 2d$. Let $K/\mathbf{Q}_p$ be an unramified extension with $\mathcal{O}$ the ring of integers of K and write $f = [k : \mathbf{F}_p]$ for the degree of the field extension $k/\mathbf{F}_p$. Then the groups $\mathrm{SL}^1_d(\mathcal{O})$ and $\mathrm{SL}^1_d(\mathbf{F}_{p^f}[\![T]\!])$ have the same normal subgroup zeta function.*

Hence the groups $\mathrm{SL}^1_d(\mathcal{O})$ and $\mathrm{SL}^1_d(\mathbf{F}_{p^f}[\![T]\!])$ in the corollary are two examples of *normally isospectral* groups.

In order to compute the normal zeta function of the groups $\mathrm{SL}^1_d(\mathcal{O})$ explicitly, we need to understand the behaviour of the map

$$V \mapsto \delta_K V + [\mathfrak{sl}_d(k), V]$$

where V is a subspace of $\mathfrak{sl}_d(k)$. We need to know for all integers $1 \leq m, n \leq d^2 - 1$ how many subspaces V of $\mathfrak{sl}_d(k)$ there are satisfying

$$\dim_{\mathbf{F}_p} V = m \quad \text{and} \quad \dim_k(\delta_K V + [\mathfrak{sl}_d(k), V]) = n.$$

These computations are done in Section 5.4. Using these computations we derived the normal zeta function of the groups $\mathrm{SL}^1_2(\mathbf{Z}_p)$ $(p > 2)$, $\mathrm{SL}^1_3(\mathbf{F}_p[\![T]\!])$ and $\mathrm{SL}^1_3(\mathbf{Z}_p)$ $(p > 3)$. We also recover the same normal zeta function for the group $\mathrm{SL}^1_2(\mathbf{F}_p[\![T]\!])$ as in [58].

Theorem 1.0.10. *Let $p > 2$ be a prime number. The normal zeta function of the group $\mathrm{SL}^1_2(\mathbf{Z}_p)$ is given by*

$$\zeta^{\triangleleft}_{\mathrm{SL}^1_2(\mathbf{Z}_p)}(s) = 1 + \frac{(p^2 + p + 1)t}{1 - t}, \quad t = p^{-s}$$

and hence for any $m \in \mathbf{N}$ we have $a^{\triangleleft}_{p^m}(\mathrm{SL}^1_2(\mathbf{Z}_p)) = p^2 + p + 1$.

Consequently, the normal subgroup growth of the group $\mathrm{SL}^1_2(\mathbf{Z}_p)$ for $p > 2$ is given by

$$s^{\triangleleft}_{p^n}(\mathrm{SL}^1_2(\mathbf{Z}_p)) = 1 + n(p^2 + p + 1), \quad n \in \mathbf{N}.$$

Theorem 1.0.11. *Let $p > 3$ be a prime number. The normal zeta functions of the groups $\Gamma_0 = \mathrm{SL}^1_3(\mathbf{F}_p[\![T]\!])$ and $\Gamma_1 = \mathrm{SL}^1_3(\mathbf{Z}_p)$ are of the form*

$$\zeta^{\triangleleft}_{\Gamma_\ell}(s) = \frac{1 + a^\ell_1(p)t + \ldots + a^\ell_{11}(p)t^{11}}{1 - t^8}$$

where $t = p^{-s}$, $\ell \in \{0, 1\}$ *and* $a_i^\ell(X) \in \mathbf{Z}[X]$ *are polynomials in* X *with non-negative coefficients. Write* $\mathbf{a}_\ell = (\deg a_1^\ell(X), \ldots, \deg a_{11}^\ell(X))$ *for the list of degrees of the polynomials* $a_1^\ell, \ldots, a_{11}^\ell$. *We then have*

$$\mathbf{a}_0 = (7, 12, 15, 16, 15, 12, 10, 10, 10, 10, 8)$$

and

$$\mathbf{a}_1 = (7, 12, 15, 16, 15, 12, 9, 8, 9, 9, 7).$$

The explicit polynomials a_i^ℓ can be found in Section 5.6.7. The difference between the two sequences $\mathbf{a}_0, \mathbf{a}_1$ is explained by the fact that the condition $V + [L, V] \subseteq W$ is more restrictive than the condition $[L, V] \subseteq W$.

Chapter 2

Preliminaries

In this chapter we recall some well-known definitions and useful results. We need this for the later chapters.

Global fields and local fields

We give a brief overview of global fields and local fields. *Global fields* are either number fields, i.e. finite field extension of the field $\mathbf{Q}$ of rational numbers, or function fields in one variable over a finite field, i.e. a finite extension of $\mathbf{F}_p(T)$ for some prime number p. *Local fields* are either Archimedean, in which case they are $\mathbf{R}$ or $\mathbf{C}$, the fields of real and complex numbers, or non-Archimedean, in which case they are finite extensions of the fields $\mathbf{Q}_p$ or finite extensions of the fields $\mathbf{F}_p(\!(T)\!)$ for some prime number p. For more on global fields and local fields see [40, Ch. 25]. We will fix the notation for these fields for the remainder of this thesis.

For a non-Archimedean local field K let $\mathcal{O}$ denote the ring of integers of K. Write $\mathfrak{p}$ for the unique maximal ideal of $\mathcal{O}$ and q for the cardinality of the finite residue field $\mathcal{O}/\mathfrak{p} \cong \mathbf{F}_q$. Moreover, let $v = v_\mathfrak{p} : K \to \mathbf{Z} \cup \{\infty\}$ be the discrete valuation on K with $v(\mathfrak{p} \backslash \mathfrak{p}^2) = 1$ and write $|\cdot|_\mathfrak{p}$ for the induced absolute value on K satisfying $|x|_\mathfrak{p} = q^{-v(x)}$ for all $x \in K$.

For a global field K let $\mathcal{O}$ denote the ring of integers of K. For a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ we denote by $K_\mathfrak{p}$ the completion of the field K with respect to the ideal $\mathfrak{p}$. This field $K_\mathfrak{p}$ is a non-Archimedean local field. We write $\mathcal{O}_\mathfrak{p}$ for the ring of integers of the field $K_\mathfrak{p}$ and

$\mathfrak{p}\mathcal{O}_\mathfrak{p}$ for the unique maximal ideal of $\mathcal{O}_\mathfrak{p}$.

When K is a global field or a non-Archimedean local field, its ring of integers $\mathcal{O}$ is a Dedekind domain. We write $|.|$ for the ordinary absolute value on the fields $\mathbf{R}$ or $\mathbf{C}$. For a non-Archimedean local field K and an integer $d \in \mathbf{N}$ we extend the discrete valuation v on K to $\mathrm{Mat}_d(K)$, the $d \times d$-matrices with entries in K, by defining

$$v(x) = \min_{1 \leq i,j \leq d} v(x_{ij})$$

for $x = (x_{ij}) \in \mathrm{Mat}_d(K)$.

Example 2.0.1. (a) Let p be a prime number and consider the non-Archimedean local field $\mathbf{Q}_p$ of p-adic rational numbers. The ring of integers of $\mathbf{Q}_p$ is the ring of $\mathbf{Z}_p$ of p-adic integers and the maximal ideal of $\mathbf{Z}_p$ is $p\mathbf{Z}_p$. The residue field is $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{F}_p$. We can write any non-zero element $a \in \mathbf{Q}_p$ as $a = p^n b$ for some integer $n \in \mathbf{Z}$ and some unit $b \in \mathbf{Z}_p^*$, we then have $v(p^n b) = n$ and hence the induced absolute value, which we denote by $|.|_p$, is given by $|a|_p = p^{-n}$.
(b) The ring of integers of the global field $\mathbf{Q}$ is $\mathbf{Z}$, the ordinary integers. Let p be a prime number, then $p\mathbf{Z}$ is a maximal ideal of $\mathbf{Z}$. The completion of $\mathbf{Q}$ with respect to the ideal $p\mathbf{Z}$ is the field $\mathbf{Q}_p$ of p-adic rational numbers.

When K is a number field and I a non-zero ideal of the ring of integers $\mathcal{O}$ of K, then the quotient $\mathcal{O}/I$ has finite cardinality and we write $N(I) = |\mathcal{O} : I|$ for the index. The function N on non-zero ideals of I is called the (absolute) norm and it is completely multiplicative. So for non-zero ideals I, J of $\mathcal{O}$ we have

$$N(IJ) = N(I)N(J).$$

Finitely generated modules over a Dedekind domain

In Chapter 4 we need the structure theorem for finitely generated modules over a Dedekind domain. Let R be an integral domain. We say R is a *Dedekind domain*, if the following three conditions holds: R is a Noetherian ring, R is integrally closed and every non-zero prime ideal of R is maximal. There are several other, but equivalent, definitions of a Dedekind domain.

Theorem 2.0.2. [23, p. 484–485] *Let R be a Dedekind domain and M a finitely generated module over R. There exists a unique integer $d \geq 0$ and there exist ideals $I_1, \ldots, I_k$ of R such that*

$$M \cong R^d \oplus \left(\bigoplus_{i=1}^{k} R/I_i \right).$$

Dirichlet series

To a sequence $\mathbf{a} = (a_n)_{n\geq 1}$ of complex numbers we associate the *Dirichlet series*, which is a series of the form

$$\zeta_{\mathbf{a}}(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad s \in \mathbf{C}.$$

Dirichlet series are a special type of generating series and they occur frequently in different areas of mathematics, for example in algebraic number theory or in group theory. A common theme is to relate the algebraic properties of the sequence $\mathbf{a}$ to the analytic properties of $\zeta_{\mathbf{a}}(s)$. Interesting analytic properties are, for example, (absolute) convergence, the value of the abscissa of convergence, the order and the residue at a pole. The most famous example of a non-trivial Dirichlet series is the Riemann zeta function $\zeta(s)$, defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad s \in \mathbf{C}.$$

Let $\mathbf{a} = (a_n)_{n\geq 1}, \mathbf{b} = (b_n)_{n\geq 1}$ be two sequences of complex numbers with $\zeta_{\mathbf{a}}(s), \zeta_{\mathbf{b}}(s)$ respectively their Dirichlet series. When $\zeta_{\mathbf{a}}(s), \zeta_{\mathbf{b}}(s)$ both converge on some common half-plane H and satisfy $\zeta_{\mathbf{a}}(s) = \zeta_{\mathbf{b}}(s)$ for all $s \in H$, then we have that the sequences $\mathbf{a}, \mathbf{b}$ are equal. A well-known property of the Riemann zeta function $\zeta(s)$ is the existence of an Euler product

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1-p^{-s}},$$

where the product is over all prime numbers p, as a formal identity (also both sides converge for $\mathrm{Re}(s) > 1$). In general, an Euler product for a Dirichlet series is an expansion of the Dirichlet series into a product of other Dirichlet series indexed by prime numbers or prime ideals. For instance, for a number field K its Dedekind zeta function, which is an important analytic function in number theory, is defined by

$$\zeta_K(s) = \sum_{0\neq I\subseteq \mathcal{O}} N(I)^{-s}, \quad s \in \mathbf{C},$$

where the summation is over all non-zero ideals I of $\mathcal{O}$ with $N(I) = |\mathcal{O} : I|$ its index, and it corresponds to the Dirichlet series of the sequence $(a_n)_{n\geq 1}$ with $a_n = |\{I \trianglelefteq \mathcal{O} \mid N(I) = n\}|$. The Dedekind zeta function $\zeta_K(s)$ has the Euler product

$$\sum_{0\neq I\subseteq \mathcal{O}} N(I)^{-s} = \prod_{\mathfrak{p}} \frac{1}{1-N(\mathfrak{p})^{-s}},$$

where the product runs over all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$ (both sides converge for $\mathrm{Re}(s) > 1$). The Dedekind zeta function generalises the Riemann zeta function.

We finish with an interesting theorem. For two functions $f, g : \mathbf{R}_{>0} \to \mathbf{R}_{>0}$ we write $f(x) \sim g(x)$ for $x \to \infty$, if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. We write Γ for the Gamma function defined by

$$\Gamma(s) = \int_0^\infty t^{s-1} e^{-t} \, \mathrm{d}t, \quad s \in \mathbf{C} \text{ with } \mathrm{Re}(s) > 0,$$

satisfying $\Gamma(n) = (n-1)!$ for all natural numbers $n \in \mathbf{N}$. The next theorem describes the summatory growth of the coefficients of a Dirichlet series in terms of analytic properties of the series. Its statement is a rewording of [28, Thm. 4.20].

Theorem 2.0.3. [28, Thm. 4.20] *Let* $\mathbf{a} = (a_n)_{n\geq 1}$ *be a sequence of non-negative real numbers such that the corresponding Dirichlet series*

$$\zeta_{\mathbf{a}}(s) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad s \in \mathbf{C}$$

converges on the half-plane $\mathrm{Re}(s) > a$ *for some real number* $a > 0$. *Assume that in a neighbourhood of* a *we can write*

$$\zeta_{\mathbf{a}}(s) = \frac{f(s)}{(s-a)^b} + g(s),$$

where $f(s), g(s)$ *are holomorphic;* $b > 0$ *is a positive real number and* $f(a) \neq 0$. *Assume also that* $\zeta_{\mathbf{a}}(s)$ *can be holomorphically continued to the line* $\mathrm{Re}(s) = a$, *except for the pole at* $s = a$. *Then we have for the summatory function* $S(x) = \sum_{n\leq x} a_n$, *when* x *tends to infinity, that*

$$S(x) \sim \frac{f(a)}{a\,\Gamma(b)} x^a (\log x)^{b-1}.$$

Principal congruence subgroups

In this section we introduce the principal congruence subgroups of two types of groups. We use these groups in Chapter 4 and Chapter 5. Let R be a ring (commutative with one). For an integer $d > 0$ we write

$$\mathrm{GL}_d(R) = \{x \in \mathrm{Mat}_d(R) \mid \det(x) \in R^*\}$$

for the group of all invertible $d \times d$-matrices with entries in R and we write

$$\mathrm{SL}_d(R) = \ker(\det : \mathrm{GL}_d(R) \to R^*)$$

for the special linear group of degree d over the ring R.

Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and let $\mathfrak{p}$ be the maximal ideal of $\mathcal{O}$. We write $\mathrm{GL}_d(\mathcal{O})$ for the subgroup of $\mathrm{GL}_d(K)$ consisting of the elements in $\mathrm{GL}_d(K) \cap \mathrm{Mat}_d(\mathcal{O})$ whose inverse in $\mathrm{GL}_d(K)$ also has all its entries in $\mathcal{O}$. The group $\mathrm{SL}_d(\mathcal{O})$ is defined as the kernel of the map $\det : \mathrm{GL}_d(\mathcal{O}) \to \mathcal{O}^*$. For an integer $n \in \mathbf{N}$ we define the *n-th principal congruence subgroup* $\mathrm{GL}_d^n(\mathcal{O})$ of $\mathrm{GL}_d(\mathcal{O})$ by

$$\mathrm{GL}_d^n(\mathcal{O}) = \ker(\mathrm{GL}_d(\mathcal{O}) \to \mathrm{GL}_d(\mathcal{O}/\mathfrak{p}^n)).$$

Hence $\mathrm{GL}_d^n(\mathcal{O})$ consists of all matrices in $\mathrm{GL}_d(\mathcal{O})$ which are congruent to the identity matrix modulo $\mathfrak{p}^n$. The reduction map $\mathrm{GL}_d(\mathcal{O}) \to \mathrm{GL}_d(\mathcal{O}/\mathfrak{p}^n)$ is surjective and hence we have an isomorphism

$$\mathrm{GL}_d(\mathcal{O})/\mathrm{GL}_d^n(\mathcal{O}) \cong \mathrm{GL}_d(\mathcal{O}/\mathfrak{p}^n).$$

For an integer $n \in \mathbf{N}$ we define the *n-th principal congruence subgroup* $\mathrm{SL}_d^n(\mathcal{O})$ of $\mathrm{SL}_d(\mathcal{O})$ by

$$\mathrm{SL}_d^n(\mathcal{O}) = \ker(\mathrm{SL}_d(\mathcal{O}) \to \mathrm{SL}_d(\mathcal{O}/\mathfrak{p}^n)).$$

Similarly, the reduction map $\mathrm{SL}_d(\mathcal{O}) \to \mathrm{SL}_d(\mathcal{O}/\mathfrak{p}^n)$ is surjective, giving the isomorphism

$$\mathrm{SL}_d(\mathcal{O})/\mathrm{SL}_d^n(\mathcal{O}) \cong \mathrm{SL}_d(\mathcal{O}/\mathfrak{p}^n).$$

Gaussian binomial coefficients

Let $0 \leq k \leq n$ be integers and q a variable. The Gaussian binomial coefficient $\binom{n}{k}_q$ is defined by

$$\binom{n}{k}_q = \frac{(1-q^n)(1-q^{n-1}) \cdot (1-q^{n-k+1})}{(1-q)(1-q^2)\cdots(1-q^k)}.$$

It turns out that $\binom{n}{k}_q$ is actually a polynomial in $\mathbf{Z}[q]$. Suppose q is a prime power. Let V be a vector space of dimension n over $\mathbf{F}_q$, here $\mathbf{F}_q$ is the finite field with q elements, then $\binom{n}{k}_q$ equals the number of subspaces of dimension k of V.

Chapter 3

Automorphisms of local fields

3.1 Declaration

The first part of this thesis consists of the article

Automata and finite order elements in the Nottingham group

by Jakub Byszewski, Gunther Cornelissen and myself, published in the Journal of Algebra Volume 602 (2022), pages 484–554; [14]. A link to an older version of the paper, differing only slightly from the article, can be found on the arXiv [13]. The paper was written during my time as a PhD student at the HHU Düsseldorf and originally intended as a write-up of results found during my master's thesis, at Utrecht University supervised by G. Cornelissen (2018), on the same subject [61].

During the process of writing the paper we continued to discover relevant new results and so we incorporated them into the paper. In the end, the contribution to the research and preparation of the paper was divided equally among the three authors. Some of the new results were discovered by myself during my PhD time and therefore this paper is a part of my PhD thesis. Roughly a quarter of my own contribution to the paper was done during my master's, the rest during my PhD time. The paper is a collaboration of the three authors and consequently many of the results were obtained jointly, moreover any contribution by one of us has subsequently been edited by the other two authors.

Below is a short summary of my more noteworthy contributions to the paper during my time as a PhD student.

- Section 3.2b. The analysis of the algorithm of Christol in Section 3.2b was written by me.

- Section 4. For this specific section I collaborated with Ragnar Groot Koerkamp, he is not an author of the paper, but his contribution is credited in Section 4 and in the acknowledgements. Together we developed an algorithm to produce a list of automata on at most 5 states representing series of order 2 and 4. The implementation in `C++` was done by Groot Koerkamp. This resulted in Proposition 4.2.1, that the series $\sigma_{\min}$ is the unique series of order 4 on at most 5 states.

- Proposition 5.3.1. The unique, up to conjugation, series $\sigma_{(1,9)}$ of order 4 with break sequence $(1, 9) = \langle 1, 5\rangle$ was found by me.

- Proposition 8.2.1. The explicit example of the embedding of the Klein four-group in $\mathcal{N}(\mathbf{F}_2)$ with generators $\sigma_{\mathrm{V},1}, \sigma_{\mathrm{V},2}$ was found by me.

- Proposition 9.2.1. The original proof, that the degree and height of an algebraic element of the Nottingham are equal, comes from me. The current proof is a simplification of my original proof.

- Theorem 11.2.6. Showed originally that $\sigma_{\mathrm{J}}, \sigma_{\mathrm{J}}^{\circ 3} \in \hat{\widehat{S}} \backslash \widehat{S}$ and $\sigma_{\mathrm{K},3}, \sigma_{(1,5)} \notin \hat{\widehat{S}}$. The current proof of Theorem 11.2.6 uses different methods.

- Proposition 12.2.1. I developed a criterion, verifiable on automata, for a series to not be an element of $\widehat{S}$.

My co-authors were consulted during the preparation of this statement and they have seen its final form.

Journal of Algebra 602 (2022) 484–554

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Automata and finite order elements in the Nottingham group

Jakub Byszewski [a], Gunther Cornelissen [b,*], Djurre Tijsma [c]

[a] *Wydział Matematyki i Informatyki, Uniwersytet Jagielloński, ul. S. Łojasiewicza 6, Kraków, 30-348, Poland*
[b] *Mathematisch Instituut, Universiteit Utrecht, Postbus 80.010, Utrecht, 3508 TA, The Netherlands*
[c] *Mathematisches Institut der Heinrich-Heine-Universität, Universitätsstraße 1, Düsseldorf, 40225, Germany*

ARTICLE INFO

Article history:
Received 1 October 2020
Available online 1 April 2022
Communicated by Kirsten Eisenträger

MSC:
11B85
11-04
11G20
11S31
11Y16
20E18
20E45
68Q70

Keywords:
Nottingham group
Power series over finite fields
Automata theory

ABSTRACT

The Nottingham group at 2 is the group of (formal) power series $t + a_2t^2 + a_3t^3 + \cdots$ in the variable t with coefficients a_i from the field with two elements, where the group operation is given by composition of power series. The depth of such a series is the largest $d \geqslant 1$ for which $a_2 = \cdots = a_d = 0$.

Only a handful of power series of finite order (forcedly a power of 2) are explicitly known through a formula for their coefficients. We argue in this paper that it is advantageous to describe such series in closed computational form through automata, based on effective versions of proofs of Christol's theorem identifying algebraic and automatic series.

Up to conjugation, there are only finitely many series σ of order 2^n with fixed break sequence (i.e. the sequence of depths of $\sigma^{\circ 2^i}$). Starting from Witt vector or Carlitz module constructions, we give an explicit automaton-theoretic description of: (a) representatives up to conjugation for all series of order 4 with break sequence $(1, m)$ for $m < 10$; (b) representatives up to conjugation for all series of order 8 with minimal break sequence $(1, 3, 11)$; and (c) an embedding of the Klein four-group into the Nottingham group at 2.

We study the complexity of the new examples from the algebro-geometric properties of the equations they satisfy. For

* Corresponding author.
E-mail addresses: jakub.byszewski@gmail.com (J. Byszewski), g.cornelissen@uu.nl (G. Cornelissen), tijsma@uni-duesseldorf.de (D. Tijsma).

https://doi.org/10.1016/j.jalgebra.2022.03.019

this, we generalise the theory of sparseness of power series to a four-step hierarchy of complexity, for which we give both Galois-theoretic and combinatorial descriptions. We identify where our different series fit into this hierarchy. We construct sparse representatives for the conjugacy class of elements of order two and depth $2^\mu \pm 1$ ($\mu \geqslant 1$). Series with small state complexity can end up high in the hierarchy. This is true, for example, for a new automaton we found, representing a series of order 4 with 5 states (the minimal possible number for such a series).

1. Introduction

Suppose $\sigma(t) = t + a_2t^2 + a_3t^3 + a_4t^4 + \cdots \neq t$ is a formal power series in the variable t with coefficients from the field $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$ with two elements. Since $\sigma(t) = t + O(t^2)$, substituting $\sigma(t)$ into itself produces a power series $\sigma^{\circ 2}(t) = t+a_2(a_3+1)t^4+\cdots$, and one may iterate this process to arrive at $\sigma^{\circ N}(t) := \sigma(\sigma(\cdots\sigma(t)))$. (We will systematically write $\sigma^{\circ N}(t)$ for the N-fold composition, and $\sigma(t)^N$ for the N-th power of the power series $\sigma(t)$; so here, for example, $\sigma(t)^2 = t^2 + a_2t^4 + \cdots$.) Our concern is *the explicit description of σ and N for which $\sigma^{\circ N}(t) = t$* (this is only possible if N is a power of 2). Our goal is not to compute finitely many coefficients a_i of such $\sigma(t)$, but rather to give a *finite description* of the complete series. To accomplish this, one might search for explicit formulas for the general coefficient a_i or for the set

$$E(\sigma) := \{i \in \mathbf{Z}_{\geqslant 0} : a_i \neq 0\}$$

of occurring exponents, and this has been done in a few cases. In this paper, we will argue that one may push the boundaries of what is currently feasible by describing the coefficients of the power series by means of a finite automaton (that such a description is possible was already pointed out in [9, Rem. 1.5]). We will construct the automaton using symbolic computation, based on Christol's characterisation of algebraic power series by automata [23,24]. We wish to stress that an automaton is a perfectly deterministic finite description of the corresponding power series $\sigma(t)$, but that a very small automaton (i.e. with very few states) may correspond to a power series for which an elementary description of the set $E(\sigma)$ is very complex. If one is interested in just the computation of the k-th coefficient of the power series $\sigma(t)$, the automaton can be used to do this in time logarithmic in k.

We will first review the mathematical relevance of this problem. Then we describe existing results and explain our method. Since the same question makes sense for the finite field $\mathbf{F}_p$ with p elements (where p is prime, and then forcedly N is a power of p), we will consider this more general problem in the theoretical parts of the paper.

1.1. Connections

Fixing a prime number p, the *Nottingham group* $\mathscr{N}(\mathbf{F}_p)$ is the pro-p-Sylow subgroup of the group of ring automorphisms $\mathrm{Aut}(\mathbf{F}_p[\![t]\!])$ of the formal power series ring $\mathbf{F}_p[\![t]\!]$ over the finite field $\mathbf{F}_p$, with composition as multiplication. There is a group isomorphism $\mathrm{Aut}(\mathbf{F}_p[\![t]\!]) \cong \mathscr{N}(\mathbf{F}_p) \rtimes \mathbf{F}_p^*$. A ring endomorphism σ of $\mathbf{F}_p[\![t]\!]$ is determined uniquely by the image $\sigma(t) \in t\mathbf{F}_p[\![t]\!]$ of t, and $\mathscr{N}(\mathbf{F}_p)$ is identified with the group of power series $\sigma(t) \in \mathbf{F}_p[\![t]\!]$ with $\sigma(t) = t + O(t^2)$ under composition. We write $\sigma \circ \tau$ for the result of substituting the series $\tau \in \mathscr{N}(\mathbf{F}_p)$ for the variable t in $\sigma \in \mathscr{N}(\mathbf{F}_p)$. The Nottingham group arises in many areas:

- In *group theory*, as Ershov remarked in [32], $\mathscr{N}(\mathbf{F}_p)$ is 'an excellent test example for many questions or conjectures in profinite group theory that have been settled for Chevalley groups'. In that reference, he proved that for $p \geqslant 5$, $\mathscr{N}(\mathbf{F}_p)$ admits no open embedding into a topologically simple group. On the other hand, every countably based pro-p group embeds into $\mathscr{N}(\mathbf{F}_p)$ (Camina [20]; Jennings [44]); in particular, every finite p-group embeds into $\mathscr{N}(\mathbf{F}_p)$ (an older unpublished result of Leedham-Green and Weiss; see [20, Thm. 3]).
- In *number theory*, the Nottingham group occurs naturally in the theory of wild ramification (as the group of wild automorphisms of $\mathbf{F}_p(\!(t)\!)$; see Fesenko [33]).
- The previous point relates to *algebraic geometry*, namely: if a group G acts on a smooth projective curve X over $\mathbf{F}_p$, then the stabiliser G_x of a point $x \in X$ acts on the completion of the local ring $\mathscr{O}_{X,x}$. This completion is isomorphic to $\mathbf{F}_p[\![t]\!]$, leading to an embedding of the wild ramification group G_x^1 (the p-Sylow subgroup of G_x) into $\mathscr{N}(\mathbf{F}_p)$; one can, for example, study deformations of group actions on curves through deformations of this group homomorphism, much like deformations of linear group representations, e.g. of Galois groups, cf. [56].

The need for explicit representations of finite order elements in $\mathscr{N}(\mathbf{F}_p)$ has been articulated several times, both in group theory ([21, p. 216], [54, §5.4]), as well as in deformation theory, where conclusive results about formal deformation spaces and/or lifting are only known when standard forms for the series are available [8,15,28,30,16,36].

Our results are also relevant for the *theory of automata* (that it relies upon), in particular, issues of implementation of certain algorithms for solving algebraic equations (Section 3, e.g. [14]), the enumeration of automata with specific properties (cf. Section 4), and an extension of Cobham's theory of complexity of automata/regular languages (cf. Section 10).

1.2. Review of previous work

Klopsch has proven that every element of order p in $\mathscr{N}(\mathbf{F}_p)$ is conjugate to

$$t/\sqrt[m]{1 - mat^m} = t + at^{m+1} + \cdots \tag{1}$$

for some positive integer m coprime to p and $a \in \mathbf{F}_p^*$, and that these series are mutually not conjugate [48]. The expression (1) may be readily converted into a formula for the coefficients of the corresponding power series by applying the binomial expansion (see also the discussion in Example 1.3.1).

Jean [43] and Lubin [54] indicated how to use formal groups and explicit local class field theory to describe elements of any order p^n in $\mathscr{N}(\mathbf{F}_p)$, and iterative procedures for the calculation of the coefficients of such elements were described (compare [42], [47], [10, §6]). However, the only known formulas for elements of order p^n for $n > 1$ are for $p^n = 4$ in $\mathscr{N}(\mathbf{F}_2)$, given by Jean in [42, Ch. 7], Chinburg and Symonds [22], and Scherr and Zieve (cf. [9, Rem. 1.4]). The Chinburg–Symonds example represents the action of an automorphism of order 4 on the local completed ring at zero of the supersingular elliptic curve over $\mathbf{F}_2$; compare also [9, Sect. 1], where it is argued that this is essentially the only example that can be constructed by such a method; more precisely, up to conjugation, it is the only 'almost rational' example. The final section of [42] contains another (implicit) way of describing a solution to the problem, this time by using the method of Mellin [57] to solve algebraic equations—in this case, a trinomial—using hypergeometric series (the historically not entirely accurate reference in [57] is to a monograph by Belardinelli).

The *break sequence* of $\sigma \in \mathscr{N}(\mathbf{F}_p)$ of order p^n is a refined invariant with the property that there are only finitely many conjugacy classes of elements of fixed order p^n with a given break sequence. The method of Lubin [54] can in principle be used to count that number using results from local class field theory. There is an exact characterisation of possible break sequences [54, Obs. 5]. We briefly recall the definitions.

Definition 1.2.1. The *depth* of $\sigma = \sigma(t) \in \mathscr{N}(\mathbf{F}_p)$ is $d(\sigma) := \mathrm{ord}_t(\sigma(t) - t) - 1$ (and $d(t) = \infty$), so if $\sigma(t) = t + a_k t^k + O(t^{k+1})$ with $a_k \neq 0$, then $d(\sigma) = k - 1$. The *lower break sequence* of an element $\sigma \in \mathscr{N}(\mathbf{F}_p)$ of finite order p^n is defined as

$$\mathfrak{b}_\sigma = (b_i)_{i=0}^{n-1} = (d(\sigma^{\circ p^i}))_{i=0}^{n-1}.$$

The data $\mathfrak{b}_\sigma$ correspond bijectively to the so-called *upper break sequence* $\mathfrak{b}^\sigma = \langle b^{(i)} \rangle_{i=0}^{n-1}$ that we will not define; for our purposes, it suffices to quote from [54, Def. 4] the formula that converts between lower and upper break sequences, which in our case of the cyclic group generated by σ becomes

$$b^{(0)} = b_0 \qquad \text{and} \qquad b^{(i)} = b^{(i-1)} + p^{-i}(b_i - b_{i-1}) \quad \text{for } i > 0. \tag{2}$$

We will always indicate lower sequences by ( )-brackets, and the corresponding upper sequences by ⟨ ⟩-brackets, and we will write $(b_i) = \langle b^{(i)} \rangle$ for corresponding lower and upper break sequences.

1.3. The method of construction

We will use the term *p-automaton* to describe a finite directed multigraph (allowing loops, as well as multiple edges between vertices) for which:

- vertices are labelled by elements of $\mathbf{F}_p$ ['output alphabet $\mathbf{F}_p$'];
- one vertex (the so-called *start vertex*) is additionally marked 'Start';
- each vertex has exactly p outgoing edges, each labelled by a different element of the set $\{0, 1, \dots, p-1\}$; ['input alphabet $\{0, 1, \dots, p-1\}$']
- there is a path in the automaton from the start vertex to any vertex ['accessibility'];
- an edge with label 0 always connects two vertices with the same label ['leading zeros invariance'].

In the general theory of automata, this is called a 'leading zeros invariant p-DFAO (deterministic finite p-automaton with output) with output alphabet $\mathbf{F}_p$ and all states accessible'. Vertices are also called 'states'. We omit the qualifier p when it is clear from the context.

Such an automaton produces the so-called *p-automatic sequence* $(a_k)_{k\geqslant 0}$, where a_k is the label carried by the final vertex of the walk that starts at the start vertex and follows the edges according to the successive digits of k in base p (starting from the least significant digit, also called the 'reverse/backwards reading convention', compare [5, 12.2]). The sequence $(a_k)_{k\geqslant 0}$ gives rise to the corresponding formal power series $\sum a_k t^k$ over $\mathbf{F}_p$ in the variable t. Note that the 'leading zeros invariance' property means that we can allow the base-p expansion of k to have any number of leading zeros without affecting the resulting sequence. Should an automaton contain inaccessible vertices, they may be removed together with all their connecting edges without changing the corresponding series.

Example 1.3.1. We consider Klopsch's series

$$\sigma_{\mathrm{K},3} := t/\sqrt[3]{1+t^3} = \sum_{k\geqslant 0} a_{3k+1} t^{3k+1} = t + t^4 + t^{13} + \dots \in \mathscr{N}(\mathbf{F}_2)$$

of order 2 with lower break sequence (3). The coefficients of this series can be described explicitly: a_{3k+1} is equal to the binomial coefficient $\binom{-1/3}{k}$ modulo 2. Writing $-1/3$ as a 2-adic integer $-1/3 = \sum_{k\geqslant 0} 4^k$, we get an infinite product representation

$$\sigma_{\mathrm{K},3} = t \prod_{k\geqslant 0} (1 + t^{3\cdot 4^k}),$$

which shows that $a_k = 1$ if and only if the base-4 expansion of $k-1$ contains only the digits 0 or 3. An automaton corresponding to this series is depicted in Fig. 1; one way

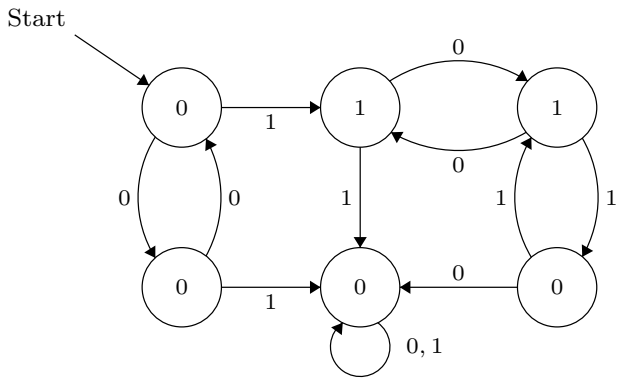


Fig. 1. A 2-automaton representing Klopsch's series $\sigma_{\mathrm{K},3} \in \mathscr{N}(\mathbf{F}_2)$ of order 2 with lower break sequence (3).

to construct it is to solve the algebraic equation $(t^3+1)\sigma^3 = t^3$ with initial coefficients $\sigma = t + t^4 + O(t^5)$ using one of the algorithms in Section 2 below.

To illustrate our reading conventions, we compute the coefficient a_{13} of the corresponding power series: write $13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$ in base 2 as 1101; begin at the start vertex and follow the directed edges with respective labels $1, 0, 1, 1$; we end up in a vertex with label 1, so $a_{13} = 1$. (If one adds leading zeros, e.g. by writing $13 = 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$, the result is the same even though the final vertex might be different.)

Our construction of elements of order p^n in $\mathscr{N}(\mathbf{F}_p)$ proceeds as follows:

(i) Use Witt vectors to construct a cyclic Galois extension of order p^n of the field of Laurent series $\mathbf{F}_p(\!(z)\!)$ with certain ramification behaviour (this is similar to the method employed by Leedham-Green and Weiss, see [20, Thm. 3]; for a discussion using class field theoretic methods instead, see Remark 2.1.2). This field extension is described in terms of a finite set of generators α_i satisfying a set of explicit algebraic relations over $\mathbf{F}_p(\!(z)\!)$ and with explicit formulas for the action of a generator σ of the Galois group on the variables α_i. Moreover, one can choose this field extension in such a way that α_i are algebraic over the field of rational functions $\mathbf{F}_p(z)$, so all computations involve algebraic functions only (cf. Examples 2.2.2 & 2.2.3).

(ii) Choose a rational function in the variables α_i that is a uniformiser for the field extension, say t. One can consider σ as an automorphism of $\mathbf{F}_p(\!(t)\!)$, and one has an explicit expression for $\sigma(t)$ as a rational function of the variables α_i. This leads to a set of algebraic equations involving $\sigma(t), t$ and α_i (note that 'algebraic' is w.r.t. the usual addition and multiplication of power series, not composition). By elimination of the variables α_i from those equations (in general with the help of a Groebner basis algorithm), one finds an explicit equation $F(t, X) = 0$ for $\sigma = \sigma(t)$ over the field $\mathbf{F}_p(t)$.

(iii) Use an algorithmic version of a proof of Christol's theorem (based on using Ore polynomials, Furstenberg's diagonal method, or differential forms on algebraic curves) to find automata whose series correspond to the solutions of the equa-

tion $F(t, X) = 0$ in $\mathbf{F}_p[\![t]\!]$. By Hensel's Lemma, sufficiently many initial coefficients of a solution will determine such a solution uniquely, so different solutions can be distinguished by solving iteratively for enough coefficients of a putative power series solution.

(iv) The equation found in (iii) might have several solutions, and at least one of these solutions is a power series of order p^n. Identify the solution(s) that correspond to elements of order p^n.

We describe the steps in some detail in the next section. In the first two steps, there are many possible choices of extensions and uniformisers, and hence there are many possible algebraic equations. The size of the resulting automaton depends heavily on the choices made in the first two steps of the method, and the minimal size of an automaton representing a power series can vary greatly in a conjugacy class (theoretical bounds depending on the equations can be found in Bridy [13]).

Once the equation is fixed, the third and fourth step in the construction (which replace the naive method of trying to solve the equation recursively for the coefficients of a putative power series solution) have been automated by Rowland (see [58] for the source code and [59] for the description) and partly in [14]; we have used these implementations to produce the automata.

1.4. Results

We start by describing the case of elements of order 4.

Theorem 1.4.1 *(Corollary 5.1.2 & Propositions 3.4.1, 4.2.1, 5.2.1, 5.3.1). The following is a complete list representing all possible elements of order* 4 *in* $\mathscr{N}(\mathbf{F}_2)$ *with break sequence* $(1, m) = \langle 1, (m+1)/2\rangle$ *for all admissible values* $m < 10$*, up to conjugation in* $\mathscr{N}(\mathbf{F}_2)$*:*

- *with break sequence* $(1, 3) = \langle 1, 2\rangle$*: two (previously known) series* σ_{CS} *and* $\sigma_{\mathrm{CS}}^{\circ 3}$ *given in Equations* (12) *&* (13)*, with the corresponding automata displayed in Table* 1*. The series* σ_{CS} *is conjugate in* $\mathscr{N}(\mathbf{F}_2)$ *to a new series* $\sigma_{\min}$ *described by the automaton in Fig.* 2*, which is the unique series of order* 4 *described by a* 2*-automaton with at most* 5 *states.*
- *with break sequence* $(1, 5) = \langle 1, 3\rangle$*: a series* $\sigma_{(1,5)}$ *corresponding to the* 13*-state automaton displayed in Fig.* 5*.*
- *with break sequence* $(1, 9) = \langle 1, 5\rangle$*: a series* $\sigma_{(1,9)}$ *with* 110*-state automaton described in Table* 2*.*

In Section 4 we present an algorithm for finding, for fixed integers N and n, all minimal 2-automata representing an element of finite order 2^n in $\mathscr{N}(\mathbf{F}_2)$ with at most N states.

For some of the automata it is possible to extract a manageable *closed formula* for the power series. We will present eight such formulas for power series of order 4 with minimal break sequence, of which five are new: $\sigma_{\mathrm{J}}^{\circ 3}$ displayed in Equations (16) & (17) and $\sigma_{\mathrm{T},1}, \sigma_{\mathrm{T},2}, \sigma_{\mathrm{T},3}$ and $\sigma_{\mathrm{T},4}$ in Table 3. Note that although it is easy to determine which of these are mutually conjugate, the conjugating power series itself may be hard to describe: as far as we know, it may be transcendental over $\mathbf{F}_2(t)$, and we are not aware of any criteria that guarantee the existence of an algebraic conjugating power series (but cf. Remark 10.2.4).

For order 8, we have the following result (for the notion of 'minimal' break sequence, see Example 2.4.3).

Theorem 1.4.2 *(Propositions 7.1.1, 7.2.1 & 7.3.1). Up to conjugation in $\mathscr{N}(\mathbf{F}_2)$, there are precisely 4 elements $\sigma_8, \sigma_8^{\circ 3}, \sigma_{8,2}, \sigma_{8,2}^{\circ 3}$ of order 8 with 'minimal' break sequence $(1,3,11) = \langle 1,2,4\rangle$ in $\mathscr{N}(\mathbf{F}_2)$, where σ_8 corresponds to the 320-state automaton given in Table 5, and $\sigma_{8,2}$ corresponds to the 926-state automaton described in 7.3.*

The automata are also stored in standard Mathematica form in [17].

Since every finite 2-group embeds in $\mathscr{N}(\mathbf{F}_2)$, Klopsch asked for a description of an embedding of the Klein four-group $V = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ in $\mathscr{N}(\mathbf{F}_2)$. We have the following result.

Theorem 1.4.3 *(Propositions 8.1.2 & 8.2.1). For every embedding of the Klein four-group V in the Nottingham group $\mathscr{N}(\mathbf{F}_2)$, some nontrivial element of V has depth at least 5. Furthermore, the series $\sigma_{V,1}$ and $\sigma_{V,2}$ corresponding to the automata depicted in Table 6 have break sequences (1) and (5) and exhibit an explicit embedding of two generators of the Klein four-group into $\mathscr{N}(\mathbf{F}_2)$.*

One notices in the examples that for fixed order and break sequence, some series with an explicit 'easy' formula are produced by a rather large automaton, while at the same time there exist series requiring fewer states for which an 'easy' formula does not seem to exist. We study this phenomenon in Section 10, generalising the concept of *sparseness*. Recall that a series $\sigma = \sum a_i t^i$ is in the class S of sparse series if the number of nonzero coefficients a_i with $i \leqslant N$ grows like a power of a logarithm of N. Klopsch's series $\sigma_{\mathrm{K},m}$ are not sparse, but at least for some values of m their conjugacy class contains a sparse series.

Theorem 1.4.4 *(Proposition 10.2.1). Any power series of order 2 and depth $m = 2^\mu \pm 1$, $\mu \geqslant 1$, is conjugate to a sparse power series $\sigma_{\mathrm{S},m}$ given in Equations (22), (23) & (24), the first two of which correspond to the automata displayed in Table 8.*

We classify general series into three classes that we consider to have 'easy formulas':

$$S \subset \widehat{S} \subset \widehat{\widehat{S}} \subset \mathbf{F}_2[\![t]\!],$$

where $\widehat{S}$ is the class of series that are sparse up to multiplication with a rational function, and $\widehat{\widehat{S}}$ is the class of series that are in $\widehat{S}$ up to composition with an automorphism of $\mathbf{F}_p(t)$. Whether or not a series is in a certain class can be studied both using Galois theory (Section 11) and combinatorics of automata (Section 12). Even for the 'larger' automata with several hundred states, the combinatorial method can be automated relatively easily using the computer algebra representation (cf. Table 11). Among the series described above there occur examples at all levels of this hierarchy of complexity.

Theorem 1.4.5 *(Theorem 11.2.6 & Table 9). The series* $\sigma_{\mathrm{T},1}, \ldots, \sigma_{\mathrm{T},4}, \sigma_{\mathrm{CS}}^{\circ 3}$ *are in* S*; the series* $\sigma_{\mathrm{CS}}, \sigma_{\mathrm{CS}}^{\circ 2}$ *are in* $\widehat{S}$ *but not in* S*; the series* $\sigma_{\mathrm{J}}, \sigma_{\mathrm{J}}^{\circ 3}$ *are in* $\widehat{\widehat{S}}$ *but not in* $\widehat{S}$*; the series* $\sigma_{\mathrm{K},m} (m \geqslant 3)$*,* $\sigma_{V,1}$*,* $\sigma_{V,2}$*,* $\sigma_{V,3}$*,* $\sigma_{\min}$*,* $\sigma_{(1,5)}$*,* $\sigma_{(1,9)}$*,* σ_8 *are not in* $\widehat{\widehat{S}}$*.*

Finally, in Section 13 we briefly discuss the synchronisation properties of some of our automata, in relation to a 'structured/random' decomposition of automatic sequences in [19].

1.5. Some open problems

- We have provided one example of an embedding of a non-cyclic p-group (the Klein four-group V) into $\mathscr{N}(\mathbf{F}_p)$ (for $p = 2$), with the break sequences of the nontrivial elements of V being (1), (1) and (5). Study the possible break sequences for embeddings of V into $\mathscr{N}(\mathbf{F}_2)$, and more generally for embeddings of arbitrary (finite) p-groups into $\mathscr{N}(\mathbf{F}_p)$ (cf. Proposition 8.1.2 and Subsection 8.3 for some explicit challenges).
- Is there a sparse series of order 2 with break sequence (11)? This is equivalent to asking whether Klopsch's series $t/\sqrt[11]{1+t^{11}} \in \mathscr{N}(\mathbf{F}_2)$ is conjugate to a sparse series. More generally, is every element of finite order in $\mathscr{N}(\mathbf{F}_2)$ sparse (or in $\widehat{S}$ or $\widehat{\widehat{S}}$) up to conjugation?
- Provide an automaton-theoretic characterisation of series that are sparse up to multiplication with a rational function, in a manner analogous to how [63] gives a necessary and sufficient condition for a series to be sparse in terms of properties of a corresponding automaton. This appears to be a hard problem, see Remark 12.2.3.
- As the automaton method allows us to extend the catalogue of known elements of finite order in $\mathscr{N}(\mathbf{F}_p)$, one may argue that it is advantageous to manipulate elements of finite order in $\mathscr{N}(\mathbf{F}_p)$ in their automatic form directly, ignoring any explicit form for the coefficients of the corresponding power series. Thus, it would make sense to study 'p-automata of finite order' as a subject of its own. How to characterise an automaton that represents a series of finite order?
- If it exists, describe an algorithm that finds all automata on at most N states that represent series of finite order. For any *given* finite order this is easy (see Section 4), so an affirmative solution of this problem would most likely require finding a bound

on the order of a series in terms of the number of states of an automaton that generates it.

Notation. We will use the notation σ and $\sigma(t)$ for elements of $\mathscr{N}(\mathbf{F}_p)$ interchangeably, and also use σ for the corresponding element of the Galois group of an extension of fields of formal Laurent series. We will also write '$\sigma(t)$' when σ is considered as an element of a Galois group and t is a specified uniformiser.

2. Detailed method: finding an algebraic equation

2.1. Extensions of Laurent series fields and elements of $\mathscr{N}(\mathbf{F}_p)$

Let $k = \mathbf{F}_p(\!(z)\!)$ be a field of formal Laurent series with corresponding valuation v_z, and let K/k be a cyclic totally ramified Galois extension of degree p^n. Let t be a uniformiser for K with corresponding valuation v_t, so that $K = \mathbf{F}_p(\!(t)\!)$. Any $\sigma \in \mathrm{Gal}(K/k)$ is an automorphism of $\mathbf{F}_p(\!(t)\!)$ fixing $\mathbf{F}_p(\!(z)\!)$, and it automatically preserves the valuation. It follows that $\sigma(t) = a_1 t + a_2 t^2 + a_3 t^3 + \cdots$ for some $a_i \in \mathbf{F}_p$; since the order of σ is a power of p, we have $a_1 = 1$, meaning that σ is an element of $\mathscr{N}(\mathbf{F}_p)$. In this way, elements of order p^n in $\mathscr{N}(\mathbf{F}_p)$ arise from totally ramified cyclic p^n-extensions of fields of Laurent series.

We first explicitly describe cyclic p^n-extensions using Witt vectors and then discuss how to detect whether they are totally ramified. By Artin–Schreier theory any abelian extension K/k of order p^n can be decomposed as a tower of field extensions

$$k = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n = K \tag{3}$$

with $K_{i+1} = K_i(\alpha_i)$ for $0 \leqslant i \leqslant n-1$ and K_{i+1}/K_i an Artin–Schreier extension with $\alpha_i^p - \alpha_i \in K_i$. In the opposite direction Witt vectors allow one to guarantee that such an iterative procedure produces a *cyclic* extension K/k.

Any $\sigma \in \mathscr{N}(\mathbf{F}_p)$ of order p^n arises from such a construction: Harbater [38, §2] proved that every such σ describes the action of a generator of the Galois group on the completed local ring at a totally ramified point of a global $\mathbf{Z}/p^n\mathbf{Z}$-Galois cover of $\mathbf{P}^1$ having a unique ramification point. The choice of a uniformiser at the ramified point (i.e. the choice of an isomorphism of the completed local ring with $\mathbf{F}_p[\![t]\!]$) corresponds to a conjugation of the representing power series. It follows that any σ of order p^n is conjugate to an algebraic power series; note that the conjugating power series is an element of $\mathscr{N}(\mathbf{F}_p)$, but is not necessarily algebraic over $\mathbf{F}_p(t)$. The genus of the cover can be computed in terms of the break sequence from the (wild) Riemann–Hurwitz formula (compare [9, §3.3 & 3.4]).

Remark 2.1.1. The general theory of Harbater–Katz–Gabber covers ([46, 1.4.1], compare [9, §4.3, Cor. 4.10]) implies that any finite subgroup of $\mathrm{Aut}(\mathbf{F}_p[\![t]\!])$ can be conjugated into a subgroup consisting of algebraic power series (but, again, the conjugating series

itself need not be algebraic). Harbater proved the result for p-groups over perfect fields. For a cohomological characterisation of the occurring Galois covers, see [50].

Remark 2.1.2. There exist alternative methods for the explicit construction of equations for the Galois extensions. One may use explicit local class field theory, using the theory of formal groups/moduli of Lubin and Tate [55]. An essentially equivalent global method is to use explicit global class field theory of function fields, employing torsion of the Carlitz module [61], and then localising at a totally ramified place. This shows, at least theoretically, that the resulting series can be described by recursion relations or automata and immediately leads to a recursive algorithm to compute the coefficients of the power series. In Remark 5.1.3 and Subsection 7.3, we describe how to find series of order 4 and 8 in this way. In particular, we use this method to construct a complete set of representatives for all conjugacy classes of order 8 elements with minimal break sequence. We have performed more experiments implementing these methods and observed that they tend to lead to automata with more states compared to the above method. A possible reason is that class field theory methods give Ore-style equations that in algorithms produce state spaces of size doubly exponential in the degree of the equation (cf. Subsection 3.3 below).

2.2. Witt vectors and construction of p^n-extensions

Let k be a field of characteristic $p > 0$ and let $n \geqslant 1$ be an integer. Let $W_n(k)$ denote the ring of (n-truncated p-typical) Witt vectors over k. As a set $W_n(k)$ is equal to k^n, and we write its elements as vectors of length n. The zero and identity element of $W_n(k)$ are $0 = (0, \dots, 0)$ and $1 = (1, 0, \dots, 0)$. Addition and multiplication of two elements $a, b \in W_n(k)$ are defined by polynomial expressions in the coordinates $a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1}$ of a and b (see e.g. Example 2.2.2 and 2.2.3 below that we will use later). The ring $W_n(k)$ comes with a Frobenius endomorphism $\mathrm{Frob}\colon W_n(k) \to W_n(k)$ mapping the element $(a_0, \dots, a_{n-1})$ to $(a_0^p, \dots, a_{n-1}^p)$. The map $\wp := \mathrm{Frob} - \mathrm{Id}$ is an endomorphism of the underlying abelian group of $W_n(k)$. Writing k^{sep} for a separable closure of k, for any given $\beta \in W_n(k)$ there exists some $\alpha \in W_n(k^{\mathrm{sep}})$ such that $\wp(\alpha) = \beta$. Such α is unique up to addition of an element of $\ker \wp = W_n(\mathbf{F}_p)$ and the extension $k(\wp^{-1}(\beta)) := k(\alpha_0, \dots, \alpha_{n-1})$ of k is independent of the choice of α. Note that $W_1(k)$ is just the field k.

Theorem 2.2.1 *(Witt; cf. [52, p. 107, Thm. 5]). Let k denote a field of characteristic $p > 0$, let k^{sep} denote a separable closure of k, and let n denote any positive integer. For any field K with $k \subseteq K \subseteq k^{\mathrm{sep}}$, K/k is a cyclic Galois extension of degree p^n if and only if there exists a $\beta \in W_n(k)$ with $\beta_0 \notin \wp(k)$ such that $K = k(\wp^{-1}(\beta))$. If $\alpha \in W_n(k^{\mathrm{sep}})$ satisfies $\wp(\alpha) = \beta$, then $k(\wp^{-1}(\beta)) = k(\alpha_0, \dots, \alpha_{n-1})$ and a generator σ of the Galois group $\mathrm{Gal}(K/k)$ is determined by the equations*

$$\sigma(\alpha_i) = (\alpha + 1)_i, \qquad i = 0, \dots, n-1. \tag{4}$$

Example 2.2.2. We consider the ring of Witt vectors $W_2(k)$ of length two over a field k of characteristic 2. For $a = (a_0, a_1), b = (b_0, b_1) \in W_2(k)$ the formulas for addition and multiplication are

$$a + b = (a_0 + b_0, a_1 + b_1 + a_0 b_0) \quad \text{and} \quad a \cdot b = (a_0 b_0, a_0^2 b_1 + a_1 b_0^2),$$

and the map $\wp$ is given by $\wp(a) = (a_0^2 + a_0, a_1^2 + a_1 + a_0^2 + a_0^3)$. Observe that this implies that $-(a_0, a_1) = (a_0, a_1 + a_0^2)$. According to Theorem 2.2.1, an extension K/k is a cyclic Galois extension of degree 4 if and only if $K = k(\alpha_0, \alpha_1)$, where α_0, α_1 satisfy

$$\begin{cases} \alpha_0^2 + \alpha_0 = \beta_0; \\ \alpha_1^2 + \alpha_1 = \beta_1 + \beta_0 \alpha_0 \end{cases}$$

for some $\beta_0, \beta_1 \in k$ with β_0 not of the form $x^2 + x$ for $x \in k$. The Galois group of K/k is generated by the field automorphism σ defined on the generators α_0, α_1 by

$$\begin{cases} \sigma(\alpha_0) = \alpha_0 + 1; \\ \sigma(\alpha_1) = \alpha_1 + \alpha_0. \end{cases} \tag{5}$$

Example 2.2.3. We consider the ring of Witt vectors $W_3(k)$ of length three over a field k of characteristic 2. For $a = (a_0, a_1, a_2), b = (b_0, b_1, b_2) \in W_3(k)$ the formula for addition is

$$a + b = (a_0 + b_0, a_1 + b_1 + a_0 b_0, a_2 + b_2 + a_1 b_1 + a_0 a_1 b_0 + a_0 b_0 b_1 + a_0^3 b_0 + a_0 b_0^3)$$

and for multiplication is

$$a \cdot b = (a_0 b_0, a_0^2 b_1 + a_1 b_0^2, a_1^2 b_1^2 + a_0^4 b_2 + a_2 b_0^4 + a_0^2 a_1 b_0^2 b_1).$$

By Theorem 2.2.1, cyclic degree-8 extensions K/k of a field k of characteristic 2 are of the form $K = k(\alpha_0, \alpha_1, \alpha_2)$, where

$$\begin{cases} \alpha_0^2 + \alpha_0 = \beta_0; \\ \alpha_1^2 + \alpha_1 = \beta_1 + \beta_0 \alpha_0; \\ \alpha_2^2 + \alpha_2 = \beta_2 + \alpha_1 \beta_1 + \alpha_0 \alpha_1 \beta_0 + \alpha_0 \beta_0 \beta_1 + \alpha_0^3 \beta_0 + \alpha_0 \beta_0^3, \end{cases} \tag{6}$$

with β_0 not of the form $x^2 + x$ for $x \in k$. The Galois group of K/k is generated by the field automorphism defined on the generators $\alpha_0, \alpha_1, \alpha_2$ by

$$\begin{cases} \sigma(\alpha_0) = \alpha_0 + 1; \\ \sigma(\alpha_1) = \alpha_1 + \alpha_0; \\ \sigma(\alpha_2) = \alpha_2 + \alpha_0 \alpha_1 + \alpha_0^3 + \alpha_0. \end{cases} \tag{7}$$

2.3. Ramification

The ramification in an Artin–Schreier extension of $\mathbf{F}_p(\!(z)\!)$ can be described using the following easy result (see e.g. [34, III.(2.5)]).

Lemma 2.3.1. *Let $k = \mathbf{F}_p(\!(z)\!)$ and let $K = k(\alpha)$ be an extension of k with $\alpha^p - \alpha = \gamma$ for some $\gamma \in k$. If $v_z(\gamma)$ is negative and not divisible by p, then K/k is a cyclic extension of degree p, and for any uniformiser π of K we have $v_\pi(\alpha) = v_z(\gamma)$; for $x \in k$ we have $v_\pi(x) = pv_z(x)$.*

If we decompose a general cyclic totally ramified p^n-extension as a tower of Artin–Schreier extensions as in (3) and we write z_i for a uniformiser of K_i (so $z_0 = z$ and $z_n = t$), then $v_{z_{i+1}}(\alpha_i) = v_{z_i}(\alpha_i^p - \alpha_i)$ for $i = 0, \dots, n-1$.

The general approach is now to take the following steps:

(i) Write down explicit equations for a cyclic p^n-extension in the variables α_i arising from the Witt construction, or other generators of the field (this may make equations simpler or help in applying Lemma 2.3.1 to check that the extension is totally ramified).
(ii) Choose a unformiser t as an algebraic function of the α_i (or the chosen field generators); using Lemma 2.3.1 allows us to control the valuations of rational functions in the field generators.
(iii) Compute the action of a generator σ of the Galois group on the uniformiser t using the action in terms of Witt vectors given by Equation (4); this gives an equation for $\sigma(t)$ in terms of the α_i (or the chosen field generators).

These three steps lead to a set of algebraic equations from which one should eliminate all but t and $\sigma(t)$, leading to an algebraic equation $F(t, X) = 0$ with $F \in \mathbf{F}_p[t, X]$ satisfied by $X = \sigma = \sigma(t)$. For elimination, one may use a Groebner basis algorithm (we used the implementation in Singular [31]; in order to be able to eliminate all the variables it might be necessary to first make a primary decomposition of the ideal generated by the equations and extract a one-dimensional component).

Example 2.3.2. We start describing what will be our 'running example' for the next few sections, leading up to a particularly small (as it will turn out, the smallest possible one in terms of number of states) automaton for a series of order 4 with 'minimal' break sequence.

Let $k = \mathbf{F}_2(\!(z)\!)$, $\beta = (z^{-1}, 0) \in W_2(k)$, and write $\alpha = (x, y) \in W_2(k^{\mathrm{sep}})$ for a solution of $\wp(\alpha) = \beta$. Since $v_z(\wp(k)) = 2\mathbf{Z} \cup \mathbf{Z}_{\geqslant 0}$ we have $z^{-1} \notin \wp(k)$, and by Theorem 2.2.1 the extension $K/k = \mathbf{F}_2(\!(z)\!)(x, y)/\mathbf{F}_2(\!(z)\!)$, with x and y satisfying

$$\begin{cases} x^2 + x = z^{-1}; \\ y^2 + y = xz^{-1} = x^3 + x^2, \end{cases}$$

is a cyclic Galois extension of degree 4. It is totally ramified; an example of a uniformiser t for K is given by

$$t = (y+1)/(y+x^2).$$

Indeed, breaking up the extension into Artin–Schreier extensions as in Equation (3), we have

$$k = K_0 = \mathbf{F}_2(\!(z_0)\!) \subsetneq K_1 = K_0(x) = \mathbf{F}_2(\!(z_1)\!) \subsetneq K_2 = K_1(y) = \mathbf{F}_2(\!(z_2)\!) = K$$

with $z_0 = z, z_1, z_2$ uniformisers of the fields in the tower of extensions. So $v_{z_0}(z^{-1}) = -1$, $v_{z_1}(x) = -1$ and $v_{z_1}(z) = 2$. Hence $v_{z_1}(x^3+x^2) = -3$, so K_1/K_0 is totally ramified. Then $v_{z_2}(y) = -3$, $v_{z_2}(x) = -2$ and $v_{z_2}(z) = 4$, so K_2/K_1 is also totally ramified. Hence t is a uniformiser for K since

$$v_{z_2}(t) = v_{z_2}(y+1) - v_{z_2}(y+x^2) = 1.$$

Formula (5) shows that a generator σ of the Galois group is determined by the equations

$$\begin{cases} \sigma(x) = x+1; \\ \sigma(y) = y+x, \end{cases}$$

the other generator is given by $\tau = \sigma^{\circ 3}$. We compute

$$\tau(t) = \sigma^{\circ 3}\left(\frac{y+1}{y+x^2}\right) = \frac{y+x}{y+x^2+x}.$$

To find an algebraic equation for $\tau = \tau(t)$ over $\mathbf{F}_2(t)$, we need to eliminate x and y from the three equations

$$\begin{cases} y^2+y = x^3+x^2 & \text{[equation of extension];} \\ (y+x^2)t = y+1 & \text{[definition of uniformiser];} \\ (y+x^2+x)\tau(t) = y+x & \text{[action of } \tau \text{ on uniformiser],} \end{cases}$$

from which we get that $X = \tau = \tau(t) \in \mathbf{F}_2[\![t]\!]$ satisfies the (irreducible) equation

$$F(t,X) = (t+1)^3X^3 + (t^3+t)X^2 + (t^3+t+1)X + t^3 + t = 0. \tag{8}$$

This equation has a unique solution of the form $t + O(t^2)$, as can be seen, e.g. from the corresponding t-adic Newton polygon; its initial coefficients are given by $t + t^2 + t^4 + t^5 + O(t^6)$.

2.4. Break sequence

By computing the first few coefficients of $\sigma \in \mathscr{N}(\mathbf{F}_p)$ of order p^n (using the algebraic equation for σ over $\mathbf{F}_p(t)$), it is easy to determine the lower break sequence of σ. If one has an explicit upper bound for the number of inequivalent series with given break sequences, we can enumerate all classes of such series by 'trying' enough equations, which sometimes works in practice. Such bounds are implicit in [54, Theorem 2.2] and have been made explicit in a few cases (cf. the discussion in Sections 5 & 7). Alternatively, using explicit local class field theory constructions as in [54] we are guaranteed to obtain representatives of all the conjugacy classes.

A method of Kanesaka and Sekiguchi directly computes the upper break sequence in terms of the Witt vector data for a given extension of $k := \mathbf{F}_p(\!(z)\!)$ [45, Thm. 5], which we rephrase as follows.

Definition 2.4.1. Fix a positive integer n. Call a vector $a = (a_i) \in \bigoplus_{\mathbf{N}} W_n(\mathbf{F}_p)$ of Witt vectors of length n (with finitely many nonzero entries) *suitable* if $a_i = 0$ for $p|i$ and for at least one i we have $a_i \in W_n(\mathbf{F}_p)^*$ (i.e. the zero component of a_i is not zero). If

$$\beta = (\beta_0, \dots, \beta_{n-1}) := \sum_{i \geqslant 0} a_i(z^{-i}, 0, \dots, 0) + \wp(b) \in W_n(k) \tag{9}$$

for a suitable $a = (a_i)$ and any $b \in W_n(k)$, define

$$\rho_n(\beta) := p^{-1} \max\{i \cdot \operatorname{ord}(a_i) : a_i \neq 0\},$$

where $\operatorname{ord}(a_i)$ is the order of a_i in the additive group $W_n(\mathbf{F}_p)$ (that itself is of exponent p^n). This is well-defined, since one can show that if a vector β admits such a representation, then the corresponding suitable vector is uniquely determined (since the vectors $(z^{-i}, 0, \dots, 0)$ are independent modulo $\wp(W_n(k))$). Also note that $\rho_n(\beta)$ is independent of $b \in W_n(k)$.

Define, for $m \leqslant n$, the truncation map $\lfloor (x_0, \dots, x_{n-1}) \rfloor_m := (x_0, \dots, x_{m-1})$. The truncation of a vector of the form as in Equation (9) in $W_n(k)$ is of that same form in $W_m(k)$.

Proposition 2.4.2 *([45]). For $k = \mathbf{F}_p(\!(z)\!)$ and a positive integer n, choose β of the form as in Equation (9) for a suitable vector $a = (a_i)$, some $b \in W_n(k)$, and assume $\beta_0 \neq 0$. Then the extension $k(\wp^{-1}(\beta))/k$ is a totally ramified cyclic extension of degree p^n, and the upper break sequence of a generator of the corresponding Galois group is $\langle \rho_1(\lfloor \beta \rfloor_1), \dots, \rho_n(\lfloor \beta \rfloor_n) \rangle$.*

Although in this paper, we usually use lower break sequences, the above result is most naturally formulated in terms of upper break sequences; as remarked before, these can be easily changed into each other using Formula (2). The above result allows one to fix

not just p^n, but also the break sequence from the start, by choosing a suitable Witt vector $\beta \in W_n(k)$. Note that we get the same extension for every $b \in W_n(k)$, but it will be convenient to rewrite certain natural choices of β using nonzero b.

Example 2.4.3. We give some examples of constructions with break sequences that we will use later.

(a) Choose $\beta = (z^{-1}, 0, \dots, 0) \in W_n(\mathbf{F}_p(\!(z)\!))$ of length n, so all $a_i = 0$ for $i \neq 1$ and $a_1 = (1, 0, \dots, 0)$. Now a_1 is of order p^n in $W_n(\mathbf{F}_p)$ and the break sequence, called the *minimal* one, is

$$\langle p^i \rangle_{i=0}^{n-1} = \left(\frac{p^{2i+1}+1}{p+1} \right)_{i=0}^{n-1}.$$

(b) For $\beta = (z^{-1}, z^{-pm}) \in W_2(\mathbf{F}_p(\!(z)\!))$, with $m > p$ coprime to p, rewrite

$$\beta = a_1(z^{-1}, 0) + a_m(z^{-m}, 0)$$

with $a_1 = (1, 0)$ and $a_m = (0, 1)$. Now $\operatorname{ord}(a_1) = p^2$ and $\operatorname{ord}(a_m) = p$ in $W_2(\mathbf{F}_p)$, so we find the upper break sequence

$$\langle 1, m \rangle = (1, pm - p + 1).$$

(c) For $\beta = (z^{-1}, z^{-m}) \in W_2(\mathbf{F}_p(\!(z)\!))$ with $m > p$ coprime to p, we get the same break sequence as the previous example, since

$$(z^{-1}, z^{-m}) = (z^{-1}, z^{-pm}) - \wp((0, z^{-m})).$$

3. Detailed method: computing p-automata using proofs of Christol's theorem

3.1. Abstract algorithm

The following theorem of Christol relates algebraic power series to p-automatic sequences (see [23,24]):

Theorem 3.1.1 *(Christol). A power series $\sigma = \sum_{k \geqslant 0} a_k t^k \in \mathbf{F}_p[\![t]\!]$ is algebraic over $\mathbf{F}_p(t)$ if and only if the sequence $(a_k)_{k \geqslant 0}$ is p-automatic.*

For our applications it is important that there are constructive proofs of this theorem: given an algebraic equation $F(t, X) = 0$ with $F(t, X) \in \mathbf{F}_p[t, X]$, the proofs can be turned into algorithms that compute p-automata representing the different solutions $X = \sigma \in \mathbf{F}_p[\![t]\!]$. These algorithms start from a finite $\mathbf{F}_p$-vector space V with a distinguished nonzero vector $s_0 \in V$ and a set Λ of 'Cartier-style' operators $\Lambda_r \colon V \to V$ for

$r \in \{0, \dots, p-1\}$. From these data, they produce the directed graph structure of an automaton. A finite computation (using Hensel's Lemma) then fills in the vertex labels for the different solutions. For three such proofs/algorithms, we briefly indicate the triples (V, s_0, Λ) and point to other sources for proofs of correctness, optimised implementations and complexity analysis.

It follows from the proofs that for a given irreducible equation all solutions can be represented by automata with the same directed graph structure (including edge labels, but excluding vertex labels). Hence the desired algorithm can be broken down into two parts: first, the computation of that directed graph, and second, computing the correct output labels corresponding to the different solutions.

We will make the following assumptions and use the following notations throughout:

- $F(t, X) \in \mathbf{F}_p[t, X]$ is irreducible,
  - $\diamond$ $d = \deg_X F$,
  - $\diamond$ $h = \deg_t F$,
  - $\diamond$ $m = \mathrm{ord}_t \mathrm{Res}_X \left(F(t, X), \frac{\partial F}{\partial X}(t, X)\right)$ denotes the t-valuation of the resultant of F and its derivative in X, and
  - $\diamond$ g denotes the geometric genus of the normalisation $\mathscr{X}$ of the projective curve corresponding to the plane affine curve $F(t, X) = 0$.
- For $0 \leqslant r < p$, the *Cartier operator* $\mathscr{C}_r$ acting on formal power series in $\mathbf{F}_p[\![x_1, \dots, x_k]\!]$ is defined by

$$\mathscr{C}_r\Big(\sum a_{i_1, i_2, \dots, i_k} x_1^{i_1} \cdots x_k^{i_k}\Big) := \sum a_{pi_1 + r, pi_2 + r, \dots, pi_k + r} x_1^{i_1} \cdots x_k^{i_k}.$$

For the first part—the construction of the directed graph underlying the automaton—the proofs are based on constructing a graph from the specific set of data (V, s_0, Λ), as follows:

⌜ **Algorithm 3.1.2** *(Labeled Directed Graph Structure).*

`Input` A finite $\mathbf{F}_p$-vector space V, $s_0 \in V$, and maps $\Lambda = \{\Lambda_r \colon V \to V \text{ for } 0 \leqslant r < p\}$.
`Output` A finite directed graph with edge labels.

Write Γ for the monoid generated by the maps Λ_r with $0 \leqslant r < p$. Compute the set of vertices S as the orbit of s_0 under the action of Γ (by applying the maps Λ_r until no new elements appear), let the vertex s_0 be labelled 'Start', and put a directed edge between s_1 and s_2 with label r precisely if $s_2 = \Lambda_r(s_1)$. ⌟

The second part can always be dealt with in the following way:

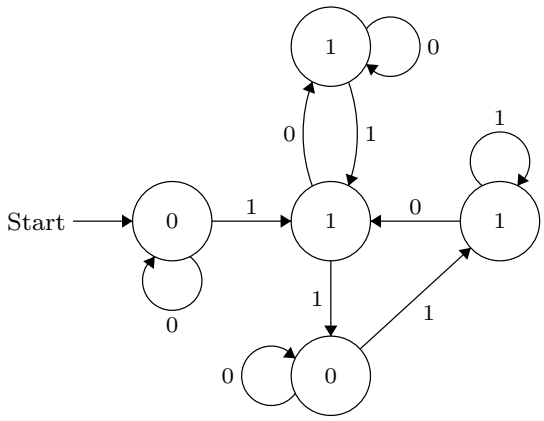


Fig. 2. A 2-automaton representing the element $\sigma_{\min}$ of $\mathscr{N}(\mathbf{F}_2)$ of order 4 with lower break sequence $(1, 3)$, corresponding to Equation (8).

⌜ **Algorithm 3.1.3** *(Vertex Labels).*

`Input` A polynomial $F(t, X) \in \mathbf{F}_p[t, X]$ and the directed graph structure, including edge labels, of automata representing all solutions $X = \sigma \in \mathbf{F}_p[\![t]\!]$ of $F(t, X) = 0$.

`Output` A finite list of automata corresponding to all these solutions.

For an integer i, consider the truncated equation

$$F(t, \sigma_0) = O(t^{i+1}) \text{ with } \sigma_0 = a_0 + a_1 t + a_2 t^2 + \cdots + a_i t^i. \tag{10}$$

(i) Solve the truncated Equation (10) with $i = 2m$ for all the (finitely many) possible σ_0. Hensel's Lemma implies that for each such σ_0 there is a unique solution $X = \sigma \in \mathbf{F}_p[\![t]\!]$ of $F(t, X) = 0$ with $\sigma(t) = \sigma_0(t) + O(t^{m+1})$ (see e.g. the introduction of [12]).

(ii) For each fixed σ_0, run through the automaton following all base-p expansions of the integers $j = 0, 1, 2, \ldots$ and give the final vertex of the walk corresponding to the base-p expansion of j the label a_j. For this, it may be necessary to compute the coefficients a_j of the solution of $F(t, X) = 0$ corresponding to σ_0 for some $j > 2m$, which can be done by solving the truncated equation inductively for $i = 2m + 1, \ldots, j$, and use the leading zeros condition. ⌟

As we will indicate below, sometimes the vertex labels can be determined in a more efficient way, depending on the method used to compute the directed graph structure.

Example (continued) 3.1.4. Suppose we know that the directed graph structure of the solutions for Example 2.3.2 is as given in Fig. 2, but the possible vertex labels are still unknown. In this case, we have $m = 6$, and we are looking for a solution σ with $\sigma = t + O(t^2)$ (already known to exist). Substituting a tentative solution, we compute its

initial coefficients: $\sigma_{\min} = t+t^2+t^4+t^5+t^7+O(t^8)$. Using the coefficients of t^0, t^1, t^3, t^7, the vertex labels are fixed uniquely, except for the label of the vertex reached from the start vertex by following the path 01. However, the assumption of leading zeros invariance fixes this value to be the same as that of the vertex reached by following the path 1. The resulting unique vertex labels are given in Fig. 2.

3.2. Three methods of constructing the input data

What is different in various proofs/algorithms is the construction of V, s_0 and Λ used as input for the construction of the directed graph. We briefly describe three possible approaches to this.

3.2.1. Using spaces of differential forms

This method is based on a proof by David Speyer and Andrew Bridy [13]. The fact that the algorithm is correct is explained in [13, §3]. A plug-and-play implementation of this algorithm is not available at the current time, but the built-in algorithms for function fields in Magma [11] include Kähler differentials and Cartier operators, making it relatively easy to implement the computations (but not the visualisations). The file [14] contains a description of a Magma routine that produces output that can be easily visualised in Mathematica and manipulated using [58].

Let Ω denote the $\mathbf{F}_p$-vector space of Kähler differentials on $\mathscr{X}$ and K the function field of $\mathscr{X}$. Writing $\eta \in \Omega$ as $\eta = (u_0^p + u_1^p t + \cdots + u_{p-1}^p t^{p-1})dt$ for unique $u_i \in K$, define the Cartier operator $\mathscr{C}\colon \Omega \to \Omega$ by the formula $\mathscr{C}(\eta) := u_{p-1}dt$. Set $\omega := Xdt \in \Omega$ and define the effective divisor $D := (\omega)_\infty + (t)_\infty$, the sum of polar divisors of the differential ω and the function t. In this case:

- $V = \Omega(D)$ is the $\mathbf{F}_p$-vector space of differential forms on $\mathscr{X}$ with divisor $\geqslant -D$ (of finite dimension $\leqslant h + 3d + g - 1$ over $\mathbf{F}_p$ by Riemann–Roch, see [13, proof of Cor. 3.10]).
- $s_0 = \omega$.
- For any $r = 0, \ldots, p-1$, define Λ_r as $\Lambda_r(\eta) := \mathscr{C}(t^{p-1-r}\eta)$. The maps Λ_r map V to itself (see [13, proof of Cor. 3.10]).

Example (continued) 3.2.1. Continuing the previous Example 2.3.2, we find (using Magma) that the curve corresponding to Equation (8) is of genus $g = 1$, the space $\Omega((Xdt)_\infty + (t)_\infty)$ is of dimension 8 and the subset $S = \Gamma(Xdt)$ has 5 elements corresponding to the vertices in the automaton. Representing these by the vectors

$$S = \{(1,1,0,1,0,0,1,0), (1,0,0,0,0,0,0,0), (0,1,0,0,0,0,1,0),$$
$$(1,1,0,1,0,0,0,0), (1,0,0,0,0,1,0,0)\},$$

where the third vector is the start vertex, the action of the operators Λ_0 and Λ_1 is given by right multiplication with the following explicit 8×8 matrices over $\mathbf{F}_2$:

$$\Lambda_0 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \text{ and } \Lambda_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The resulting automaton is the one in Fig. 2.

3.2.2. Using equations in Ore form

This method is based on the proof from [24]. The fact that the algorithm is correct follows, e.g. from tracing through the proof of Christol's theorem in [5, Thm. 12.2.5] using [5, 12.2.4] for the expression for the corresponding p-kernel and the construction of the automaton corresponding to such a kernel as in the proof of the equivalence of 'p-automatic' and 'finite p-kernel', see e.g. [5, Thm. 6.6.2]. (The vector space described there is slightly larger, but the arguments show that the space defined below also works.) An implementation is described in [60, Rem. 4.7] and an actual implementation was done by Rowland in [58] (compare [59]).

One first computes a new polynomial $G(t, X) \in \mathbf{F}_p[t, X]$ in 'Ore form', i.e. $G(t, X) = \sum_{i=0}^{d} B_i X^{p^i}$ with $B_i \in \mathbf{F}_p[t], B_0 \neq 0$, whose solution set in X contains the $\mathbf{F}_p$-vector space spanned by the solution set of F in X. Then the data are defined as follows:

- V is the set of linear combinations of elements from $\{X, X^p, \dots, X^{p^{d-1}}\}$ with coefficients being elements from $\mathbf{F}_p[t]$ of degree at most

$$N := \max(\deg B_0, \max\{\left\lceil \frac{\deg B_i + (p^i - 2)\deg B_0}{p-1} \right\rceil - 1 \mid 1 \leqslant i \leqslant d\}).$$

- $s_0 := B_0 X$.
- For $0 \leqslant r < p$ and $D_k \in \mathbf{F}_p[t]$ of degree at most N, define

$$\Lambda_r \left(\sum_{k=0}^{d-1} D_k X^{p^k} \right) := \sum_{k=1}^{d-1} \mathscr{C}_r(D_k - D_0 B_k B_0^{p^k - 2}) X^{p^{k-1}} - \mathscr{C}_r(D_0 B_d B_0^{p^d - 2}) X^{p^{d-1}}.$$

The bound N on the degrees of D_k is chosen so that s_0 belongs to V and the operators Λ_r map V to itself (for this, note that for a polynomial $D \in \mathbf{F}_p[t]$ we have $\deg \mathscr{C}_r(D) \leqslant \lfloor \frac{\deg D}{p} \rfloor$).

One may circumvent the use of Algorithm 3.1.3: for the solution σ_0 whose truncation was fixed in (10) (with $\ell := \operatorname{ord}_t B_0 \geqslant 1$) we can directly compute the labels of the vertices, as follows. Write

$$\frac{\sigma_0}{B_0} = b_1 t^{-(\ell-1)} + b_2 t^{-(\ell-2)} + \cdots + b_{\ell-1} t^{-1} + b_\ell + O(t) \tag{11}$$

with $b_i \in \mathbf{F}_p$; then the vertex corresponding to $\sum_{k=0}^{d-1} D_k X^{p^k} \in V$, where $D_k = \sum_{j \geqslant 0} [D_k]_j t^j$ with $[D_k]_j \in \mathbf{F}_p$, has vertex label equal to $\sum_{k=0}^{d-1} \sum_{\substack{0 \leqslant i \leqslant N \\ p^k | i}} [D_k]_i \cdot b_{\ell - i/p^k}$.

Example (continued) 3.2.2. The series τ from the previous Example 2.3.2 satisfies the following equation in Ore form:

$$G(t, X) = (t^8+1)X^8 + (t^8+t^4+t^2+1)X^4 + (t^7+t^6+t^5+t^4+t^2)X^2 + (t^7+t^5)X = 0.$$

Now $\dim V = 150$ and S consists of the following five elements, resulting in the automaton in Fig. 2:

$$\begin{aligned}
s_0 &= (t^7+t^5)X, \\
s_1 &= (t^6+t^3)X + (t^{14}+t^{13}+t^{11}+t^{10}+t^9+t^7)X^2 \\
&\qquad + (t^{28}+t^{27}+t^{26}+t^{25}+t^{20}+t^{19}+t^{18}+t^{17})X^4, \\
s_2 &= (t^7+t^6+t^5)X + (t^{13}+t^{11}+t^{10}+t^8)X^2 + (t^{28}+t^{26}+t^{20}+t^{18})X^4, \\
s_3 &= t^2 X + (t^{13}+t^8+t^7+t^6)X^2 + (t^{26}+t^{24}+t^{18}+t^{16})X^4, \\
s_4 &= (t^6+t^4)X.
\end{aligned}$$

3.2.3. Using diagonals of two-variable power series

This method splits the problem into two cases ('non-singular' and 'general') and is based on a theorem of Furstenberg [35, Prop. 2] in combination with the proof in [23] and an observation in [2]. In the special case, the algorithm is described in [60, Algorithms 1 & 2]. The general algorithm is implemented in [58]. It is somewhat different from the preceding two methods: the non-singular case follows the setup considered before, in that it produces a triple (V, s_0, Λ). The general case, however, might produce a different automaton for every solution.

Special case. Suppose $G \in \mathbf{F}_p[t, X]$ is *non-singular*, meaning that $G(0,0) = 0$ and $c := \partial G/\partial X(0,0)$ is nonzero. We search solutions $\sigma \in \mathbf{F}_p[\![t]\!]$ of $G(t, \sigma) = 0$ with $\sigma(0) = 0$. In this case, by Hensel's lemma, there is a *unique* such solution σ; Furstenberg's theorem says that

$$\sigma(t) = \Delta\left(\frac{P(t,X)}{Q(t,X)}\right)(t) \quad \text{with } P(t,X) := c^{-1}X\frac{\partial G}{\partial X}(tX,X) \text{ and}$$
$$Q(t,X) := c^{-1}X^{-1}G(tX,X),$$

where the *diagonal* ΔG of a two-variable power series $G(t,X) = \sum a_{r,s}t^r X^s \in \mathbf{F}_p[\![t,X]\!]$ is defined as the one-variable power series $(\Delta G)(t) := \sum a_{r,r}t^r \in \mathbf{F}_p[\![t]\!]$. To avoid confusion: in the definition of P, the derivative is that of $G(t,X)$ w.r.t. X, after which the result is evaluated at (tX,X), and the constant c^{-1} is introduced so that $Q(0,0) = 1$. The relevant data are:

- V is the space of polynomials in $\mathbf{F}_p[t,X]$ of degree at most $\max(\deg_t P, \deg_t Q)$ in t and of degree at most $\max(\deg_X P, \deg_X Q)$ in X.
- $s_0 := P(t,X)$.
- For $0 \leqslant r < p$, $\Lambda_r(s) := \mathscr{C}_r(sQ^{p-1})$.

In this case, Algorithm 3.1.3 may be avoided: $v \in V$ is a two-variable polynomial, and the corresponding (unique) vertex label is the value of this polynomial at $(0,0)$.

General case. Following [2, §3.1], compute the finite list of all possible polynomials $q \in \mathbf{F}_p[t]$ of degree $\leqslant 2m$ such that $F(t,q(t)) = O(t^{2m+1})$. For each such q, set $s = m + \mathrm{ord}_t(\frac{\partial F}{\partial X}(t,q(t)))$, $G(t,X) = t^{-s}F(t,t^mX + q(t))$. Now G is non-singular; apply the previous case to construct an automaton for the (unique) power series solution $\tau(t)$ of $G(t,X) = 0$ with $\tau(0) = 0$. Modify the automaton producing τ to an automaton producing a power series solution $\sigma = q + t^m\tau$ of $F(t,X) = 0$ using standard constructions with automata (see e.g. [5, Thm. 5.4.1 & Cor. 6.8.5], which have constructive proofs).

Example (continued) 3.2.3. For Example 2.3.2, the polynomial is non-singular and we have

$$P(t,X) = t^3X^6 + t^2X^5 + (t^3+t)X^4 + X^3 + tX^2 + X,$$
$$Q(t,X) = t^3X^5 + \left(t^3+t^2\right)X^4 + \left(t^3+t\right)X^3 + \left(t^3+t+1\right)X^2 + tX + t + 1.$$

The space V is of dimension 28 and V consists of 6 elements:

$$s_0 = P = t^3X^6 + t^2X^5 + (t^3+t)X^4 + X^3 + tX^2 + X,$$
$$s_1 = \Lambda_0(s_0) = t^3X^5 + (t^3+t)X^3 + tX,$$
$$s_2 = \Lambda_1(s_0) = t^2X^4 + t^2X^3 + (t+1)X^2 + tX + 1,$$
$$s_3 = \Lambda_0(s_2) = t^2X^4 + X^2 + 1,$$
$$s_4 = \Lambda_1(s_2) = t^2X^4 + (t^2+t+1)X^2 + X,$$
$$s_5 = \Lambda_1(s_4) = t^2X^4 + (t^2+1)X^2 + 1,$$

with

$$\Lambda_0(s_1)=s_1,\ \Lambda_1(s_1)=s_2,\ \Lambda_0(s_3)=s_3,\ \Lambda_1(s_3)=s_2,\ \Lambda_0(s_4)=s_4,\ \Lambda_0(s_5)=s_2,\ \Lambda_1(s_5)=s_5.$$

This leads to an automaton with 6 states, but the states corresponding to s_0 and s_1 have the same outgoing edges and the same output labels, and hence can be merged into one state without affecting the automatic sequence produced by the automaton. Doing so leads again to the automaton in Fig. 2.

3.3. Bounds on the complexity

The exact complexity of the algorithms does not appear to be known, but upper bounds on the number of states $\#S$ have been given in terms of d and h. In essentially all the known examples, these are obtained by first bounding the dimension of the vector space V, and then using the trivial inequality $\#S \leqslant p^{\dim V}$. In practice, it is often the case that the set S is much smaller than the vector space V (as seen, e.g. in Examples 3.2.1–3.2.3). We will show in Proposition 9.2.1 that $d = h$ for series of finite compositional order, and then we have the following upper bounds:

- Differential forms: $\log_p \#S \leqslant 4d + g - 1 \leqslant d(d+2) \approx d^2$ ([13, Cor. 3.10] and the inequality $g \leqslant (d-1)(h-1)$ of Castelnuovo–Riemann [62, Cor. 3.11.4]);
- Ore polynomials: $\log_p \#S \leqslant d^3 p^d (p^d - 1)/(p-1) \approx d^3 p^{2d-1}$ (using the upper bound dhp^d for the height of the Ore form equation from [1, Lem. 8.1]);
- Diagonals (non-singular case): $\log_p(\#S - 1) \leqslant d(d+1) \approx d^2$ (for this bound it is shown that all states in S except possibly for s_0 lie in a vector subspace of V of dimension $d(h+1)$ [60, Rem. 4.7], [3, Thm. 3.1]; the latter reference also contains an argument that shows that in the general case, the diagonal method gives a similar upper bound asymptotically in d as the differential forms method).

In our running example, $\#S$ is 5 or 6, and the respective bounds on $\#S$ are $2^{12}, 2^{1512}$ and $2^{12}+1$. For more information on the exact complexity of our examples (that appear to require far fewer states than the theoretical general bounds), we refer to Section 9.

3.4. Our application

Our construction using Witt vectors produces a polynomial $F(t, X) \in \mathbf{F}_p[t, X]$ of which we first check irreducibility (if the polynomial were not irreducible, we would factor it and work with the factors). We know the polynomial has at least one solution $\sigma(t) = t + O(t^2) \in \mathbf{F}_p[\![t]\!]$, and we search only for such solutions. Most of the time, we can prove that there will be a unique solution of this form, and we then know that this σ has the desired finite order under composition. In some cases, we find more than one solution, but in these cases, we can identify the correct series in a different way. For actual computations, we relied on implementations of all three algorithms; see the

section 'How computations and visualisations were done' at the end of the paper for details.

The results obtained in our running Example 2.3.2, 3.1.4, and either one of 3.2.1, 3.2.2 or 3.2.3 may be summarised as follows:

Proposition 3.4.1. *The series $\sigma_{\min}$ corresponding to the automaton in Fig. 2 is of order 4 in $\mathscr{N}(\mathbf{F}_2)$ and has break sequence $(1,3)$ and initial coefficients $\sigma_{\min} = t + t^2 + t^4 + t^5 + O(t^6)$.* □

A given finite order element of the Nottingham group can have in its conjugacy class many algebraic power series, which satisfy polynomial equations of various degrees. It would be interesting to find a theoretical upper bound on the minimal degree d of such a polynomial. This would also give an upper bound on the genus g of the curve $\mathscr{X}$ (see Subsection 3.3).

4. An enumeration algorithm for automata on at most N states representing finite order series

4.1. An abstract algorithm

Before we start applying our construction in concrete cases, we discuss an enumeration algorithm for finding all 'small' (in terms of number of states) minimal automata representing an element in $\mathscr{N}(\mathbf{F}_2)$ of given finite order. The theoretical algorithm, which can readily be generalised to p-automata and order p^n elements in $\mathscr{N}(\mathbf{F}_p)$, consists of two parts.

⌜ **Algorithm 4.1.1** *(Compositional Power Automaton).*

`Input` A 2-automaton A and an integer $n \geqslant 0$.
`Output` If σ denotes the series corresponding to A, a 2-automaton A_n corresponding to the series $\sigma^{\circ 2^n}$.

(i) Find a polynomial $F(t,X) \in \mathbf{F}_2[t,X]$ with $F(t,\sigma) = 0$. This can be done by following the proof of Christol's Theorem 3.1.1 (in the direction different from the one used in Section 3)—from the automaton, determine the 2-kernel using [5, Thm. 6.6.2] and then follow the first part of the proof in [5, Thm. 12.2.5].
(ii) Composing with $\sigma(t)$ on the right gives $F(\sigma(t), \sigma^{\circ 2}(t)) = 0$. Eliminate Y from $F(t,Y) = F(Y,X) = 0$ to produce an algebraic equation $F_1(t,X) = 0$ satisfied by $X = \sigma^{\circ 2}$. Repeat this procedure to produce an algebraic equation $F_n(t,X) = 0$ for $\sigma^{\circ 2^n}$.
(iii) Construct an automaton A_n for $\sigma^{\circ 2^n}$ from the equation $F_n(t,X) = 0$, using the methods of Section 3. ⌟

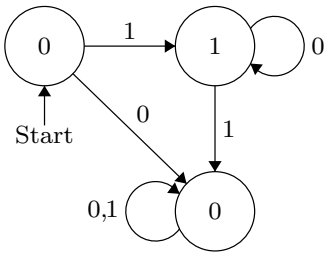


Fig. 3. Automaton for the power series t.

We will use the well-known fact that to each automaton A corresponds a unique minimal deterministic finite automaton $\widehat{A}$ with the same corresponding series, and that $\widehat{A}$ can be computed from A by an algorithm, see e.g. [51, §2.4]. In particular, one can check by an algorithm whether or not two automata A and B correspond to the same series—this happens precisely when $\widehat{A} = \widehat{B}$.

⌜ **Algorithm 4.1.2** *(Enumeration Bounded Size Automata of Fixed Compositional Order).*

`Input` Integers $n \geqslant 0$ and $N \geqslant 1$.
`Output` A finite list of all minimal 2-automata on at most N states representing an element of finite order 2^n in $\mathscr{N}(\mathbf{F}_2)$.

(i) Go over all 2-automata on at most N states and eliminate those for which the corresponding power series is not of the form $\sigma = t + O(t^2)$.
(ii) Remove duplicates from the list by comparing their minimal automata.
(iii) For each remaining automaton A use Algorithm 4.1.1 to compute the automaton A_n.
(iv) Compute the minimal automaton $\widehat{A}_n$ corresponding to A_n and check whether it equals the 3-state minimal automaton generating the series t, depicted in Fig. 3. ⌟

We do not know of an algorithm that lists all automata of size at most N corresponding to series of arbitrary but finite compositional order.

4.2. A practical implementation with application

A practical implementation of a more optimal algorithm in C++ was given by Groot Koerkamp [37] and produces a list of candidates for automata on at most 5 states representing series of order 2 and 4. Running that algorithm, we find a unique candidate automaton corresponding to a series of order 4. Since we already know from Proposition 3.4.1 that $\sigma_{\min}$ is an order-4 series which is represented by an automaton with 5 states, this proves the following.

Proposition 4.2.1 *(Groot Koerkamp, [37]). The* unique *minimal (leading zeros invariant)* 2*-automaton* with at most 5 states *representing a power series of compositional order* 4 *is the one corresponding to the series* $\sigma_{\min}$ *and depicted in Fig. 2.* □

5. Construction and classification of some order-4 elements

5.1. Order 4, break sequence $(1,3) = \langle 1,2\rangle$

Below are two known explicit power series with this order and break sequence: the one discovered by Chinburg and Symonds [22] and its compositional inverse, computed by Scherr and Zieve [9, Remark 1.4]:

$$\sigma_{\mathrm{CS}} := t + t^2 + \sum_{k\geqslant 0}\sum_{\ell=0}^{2^k-1} t^{6\cdot 2^k+2\ell} = t + t^2 + O(t^6); \tag{12}$$

$$\sigma_{\mathrm{CS}}^{\circ 3} = \sum_{k\geqslant 0}\left(t^{3\cdot 2^k-2} + t^{4\cdot 2^k-2}\right) = t + t^2 + t^4 + O(t^6). \tag{13}$$

An unpublished result of Lubin ([53], see [41, Thm. 2.2] for a proof) implies that there are precisely two conjugacy classes of such elements in $\mathscr{N}(\mathbf{F}_2)$. We now present a slightly more detailed lemma that allows us to distinguish between these conjugacy classes based on the first few coefficients alone.

Lemma 5.1.1. *Let* $\sigma \in \mathscr{N}(\mathbf{F}_2)$ *be an automorphism of order* 4 *with break sequence* $(1,3) = \langle 1,2\rangle$*, and write* $\sigma = \sum_{i=1}^{\infty} a_i t^i$ *with* $a_i \in \mathbf{F}_2$*. Then* $a_1 = a_2 = 1$*,* $a_3 = 0$*, and exactly one of the following cases holds*:

(a) $a_4 = a_5$ *and* σ *is conjugate to* σ_{CS};
(b) $a_4 \neq a_5$ *and* σ *is conjugate to* $\sigma_{\mathrm{CS}}^{\circ 3}$.

Proof. We have $a_1 = 1$ since $\sigma \in \mathscr{N}(\mathbf{F}_2)$, and $a_2 = 1$, $a_3 = 0$ since σ has lower break sequence $(1,3)$; for the latter statement, compute the power series $\sigma^{\circ 2} = t + (1+a_3)t^4 + O(t^5)$. The only possibilities for such series up to $O(t^6)$ are hence the four truncated series $\sigma = t + t^2 + a_4 t^4 + a_5 t^5 + O(t^6)$ with $a_4, a_5 \in \mathbf{F}_2$. Two of these correspond to (12) and (13), and for the other two, we observe that conjugating by $\phi : t \mapsto t + t^3$ gives

$$\phi^{-1} \circ \sigma_{\mathrm{CS}} \circ \phi = t + t^2 + t^4 + t^5 + O(t^6);$$
$$\phi^{-1} \circ \sigma_{\mathrm{CS}}^{\circ 3} \circ \phi = t + t^2 + t^5 + O(t^6).$$

The quoted result of Lubin in [41, Thm. 2.2] implies that there are precisely two conjugacy classes of power series with break sequence $(1,3) = \langle 1,2\rangle$. To finish the proof it is therefore enough to show that any automorphisms $\sigma, \tau \in \mathscr{N}(\mathbf{F}_2)$ with

$$\sigma = t + t^2 + O(t^6) \qquad \text{and} \qquad \tau = t + t^2 + t^4 + O(t^6)$$

are not conjugate in $\mathscr{N}(\mathbf{F}_2)$. Suppose this is the case, and let $\psi \in \mathscr{N}(\mathbf{F}_2)$ be such that $\sigma \circ \psi = \psi \circ \tau$. This implies that

$$\psi(t) + \psi(t)^2 + O(t^6) = \psi(t + t^2 + t^4) + O(t^6). \tag{14}$$

Writing $\psi(t) = t + \sum_{i=2}^{\infty} b_i t^i$ with $b_i \in \mathbf{F}_2$ and comparing the coefficients of t^4 and t^5 in (14) gives

$$b_2^2 + b_4 = 1 + b_2 + b_3 + b_4 \qquad \text{and} \qquad b_5 = b_3 + b_5,$$

which gives a contradiction since $b_2 \in \mathbf{F}_2$. □

Corollary 5.1.2. *The series σ_{CS} and $\sigma_{\mathrm{CS}}^{\circ 3}$ form a full set of representatives for the conjugacy classes of elements of order 4 with break sequence $(1,3) = \langle 1,2\rangle$ in $\mathscr{N}(\mathbf{F}_2)$.* □

The following different power series of order 4 and break sequence $(1,3)$ was found earlier by Jean in [42] as a solution to the equation $(t+1)\sigma^2 + (t^2+1)\sigma + t = 0$:

$$\sigma_{\mathrm{J}} := \sum_{k \geqslant 0} \frac{t^{2^k}}{(t+1)^{3\cdot 2^k - 1}} = t + t^2 + t^5 + O(t^6). \tag{15}$$

Lemma 5.1.1 implies that it is conjugate to $\sigma_{\mathrm{CS}}^{\circ 3}$.

Let us show how the power series of Chinburg–Symonds and Jean fit into our construction, and present the corresponding automata, using the same totally ramified cyclic extension $\mathbf{F}_2(\!(z)\!)(x,y)/\mathbf{F}_2(\!(z)\!)$ of degree 4 as in Example 2.3.2, but choosing different uniformisers t.

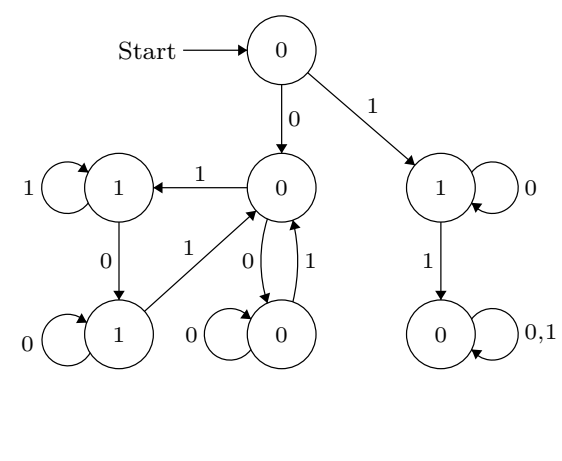
(i) First, let $t = yx^{-2}$. After elimination, we find the (irreducible) equations

$$t^2X^2 + X + t^2 + t = 0;$$
$$(t^2+1)X^2 + X + t = 0$$

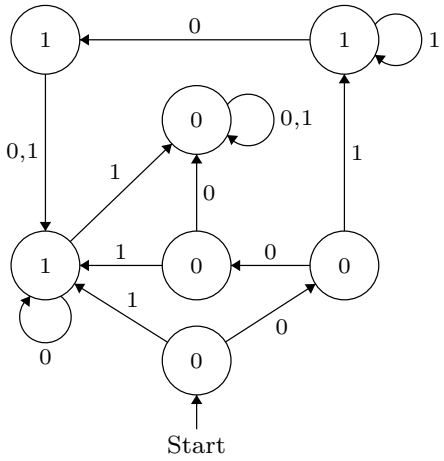
for σ and τ, respectively. Looking at the valuations of the coefficients, we see that these equations have unique solutions of the form $t + O(t^2)$. The corresponding automata are given in the top right (σ) and the top left (τ) of Table 1. We now briefly indicate how these automata can be used to construct explicit formulas for σ and τ, showing that $\sigma = \sigma_{\mathrm{CS}}^{\circ 3}$ and $\tau = \sigma_{\mathrm{CS}}$.

- Write $\tau = \sum_{i \geqslant 1} a_i t^i$ with $a_i \in \mathbf{F}_2$. We will use the automaton corresponding to τ to determine for which $i \geqslant 1$ we have $a_i = 1$. For such i, starting at the start vertex and walking through the automaton following the successive digits of i

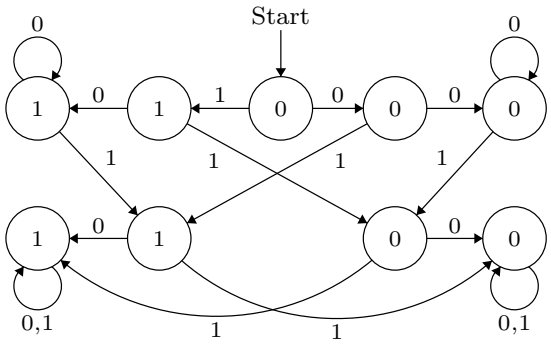
Table 1
Automata corresponding to series of Chinburg–Symonds and Jean and their inverses.



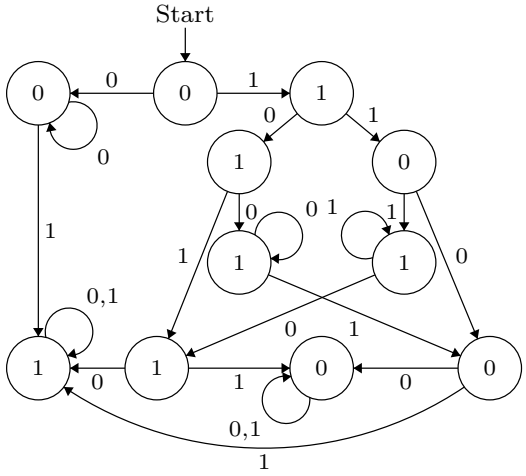
Automaton for σ_{CS}



Automaton for $\sigma_{\mathrm{CS}}^{\circ 3}$



Automaton for σ_{J}



Automaton for $\sigma_{\mathrm{J}}^{\circ 3}$

in base 2 (beginning with the least significant digit), we end up in a vertex with label 1. Since we can disregard any leading zeros, this vertex has an incoming edge with label 1. For τ note that this property holds precisely for those i for which the base-2 expansion is either 1, 10 or of the form $11d_k \cdots d_1 0$ for some $k \geqslant 0$, $d_1, \ldots, d_k \in \{0, 1\}$, i.e. for i equal to 1, 2 or such that $6 \cdot 2^k \leqslant i < 8 \cdot 2^k$ for some $k \geqslant 0$. It follows that τ is given by the formula in (12).

- For the power series $\sigma = \sum_{i \geqslant 1} b_i t^i$ we see that the positive integers i for which $b_i = 1$ are precisely those which have a base-2 expansion of the form 1, 100, $1^k 10$ or $101^k 10$ with $k \geqslant 0$, and these are exactly the base-2 expansions of the numbers 1, 4, $4 \cdot 2^k - 2$ and $12 \cdot 2^k - 2$. This proves the formula for σ given in (13).

The fact that we can find such an explicit expression appears to be quite special. This relates to the fact that the automaton is 'sparse' in the sense of Section 10 below. The automaton for τ is not sparse, but the base-2 expansion of the occurring

powers has an explicit 'closed' form. It turns out that this series is sparse up to multiplication by a rational function.

(ii) Second, let $t = xy^{-1}$. Then we find the (irreducible) equations

$$(t+1)X^2 + (t^2+1)X + t = 0;$$
$$tX^2 + (t^2+1)X + t^2 + t = 0$$

for σ and τ, respectively. From formula (15) we deduce that σ_{J} satisfies the same algebraic equation as σ, and since this equation has a unique solution of the form $t + O(t^2)$, we have $\sigma_{\mathrm{J}} = \sigma$. Solving the equations for σ and τ by automata, we find that σ correspond to the bottom left, and τ to the bottom right automaton depicted in Table 1. Converting the automata into explicit series as above, we find (after some rewriting) that

$$\begin{aligned}\sigma_{\mathrm{J}} = \sigma &= t + (t^7 + t^2)\sum_{k\geqslant 0} t^{8k} + \sum_{k,\ell\geqslant 0}\left(t^{4\cdot 2^k(4\ell+1)+1} + t^{4\cdot 2^k(4\ell+3)}\right)\\ &= t + \frac{t^7+t^2}{t^8+1} + \sum_{k\geqslant 2}\frac{t^{3\cdot 2^k} + t^{2^k+1}}{t^{4\cdot 2^k}+1},\end{aligned}$$

and

$$\begin{aligned}\sigma_{\mathrm{J}}^{\circ 3} = \tau &= t + (t^{11}+t^5)\sum_{k\geqslant 0} t^{16k} + \sum_{k\geqslant 1,\,\ell\geqslant 0}\left(t^{2^k(2\ell+1)} + t^{4\cdot 2^k(4\ell+1)-1} + t^{4\cdot 2^k(4\ell+3)+1}\right)\\ &= t + \frac{t^{11}+t^5}{t^{16}+1} + \frac{t^2}{t^2+1} + \sum_{k\geqslant 3,\,\ell\geqslant 0}\left(t^{2^k(4\ell+1)-1} + t^{2^k(4\ell+3)+1}\right). \qquad (16)\end{aligned}$$

On the other hand, from the algebraic equation for τ (which has a unique solution of the form $t+O(t^2)$), we can find directly another explicit form for τ: the series $\tilde{\tau} := \frac{t}{t^2+1}\cdot\tau$ satisfies $\tilde{\tau} = t^2/(t+1)^3 + \tilde{\tau}^2$, and hence (iteratively) $\tilde{\tau} = \sum_{k\geqslant 0}(t^2/(t+1)^3)^{2^k}$, leading to the formula

$$\sigma_{\mathrm{J}}^{\circ 3} = \tau = \sum_{k\geqslant 0}\frac{t^{2\cdot 2^k-1}}{(t+1)^{3\cdot 2^k-2}}. \qquad (17)$$

The series σ and τ are further closed forms of elements of order 4 in $\mathscr{N}(\mathbf{F}_2)$ with break sequence $(1,3)$ and conjugate to $\sigma_{\mathrm{CS}}^{\circ 3}$ and σ_{CS}, respectively.

The element $\sigma_{\min}$ in Proposition 3.4.1 is conjugate to σ_{CS}.

Remark 5.1.3. We outline a construction of an automaton for such a series of order 4 with minimal break sequence using the Carlitz module construction of abelian extensions of

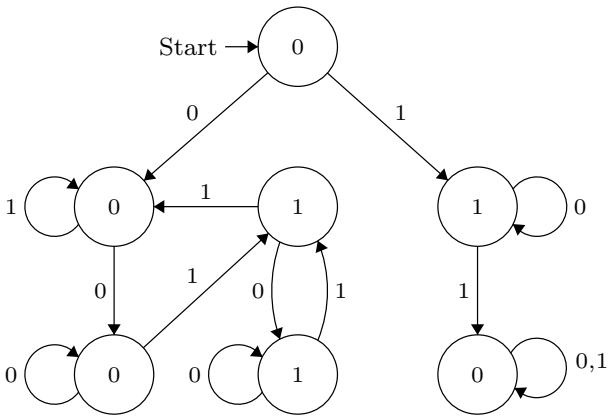


Fig. 4. Automaton corresponding to $\sigma_{\mathrm{CS}}^{\circ 2} \in \mathscr{N}(\mathbf{F}_2)$ of order 2 with break sequence (3).

function fields, see e.g. [39] (this is a global class field theory version essentially equivalent to the local method based on Lubin–Tate theory used by Jean).

Let $\rho\colon \mathbf{F}_2[z] \to \mathrm{End}(\mathbf{G}_a)$ denote the Carlitz module for $K := \mathbf{F}_2(z)$ defined by $\rho_z(X) = zX + X^2$. Now the extension $K(\rho[z^3])/K$ given by adjoining the roots of $\rho_{z^3}(X)$ is Galois with Galois group $G = \left(\mathbf{F}_2[z]/z^3\right)^* \cong \mathbf{Z}/4\mathbf{Z}$, generated by the class of $z+1$ (of order 4), where an element $g \in G$ acts on $\alpha \in K(\rho[z^3])$ by $g(\alpha) := \rho_g(\alpha)$. A minimal polynomial for the extension is $f := \rho_{z^3}(X)/\rho_{z^2}(X) = X^4 + (z^2+z)X^2 + z^2X + z$, its splitting field is a cyclic degree-4 extension in which z is totally ramified (and no other place ramifies, cf. [39, Prop. 2.2, Thm. 3.2]), and a root t is a uniformiser for the extension locally above z. The action of a generator of the Galois group is given by $\sigma(t) = \rho_{z+1}(t) = t + zt + t^2$.

Eliminating z, we find an equation $(t+1)X^2 + (t^2+1)X + t = 0$ for σ. This is exactly the equation for σ_{J}, previously obtained using Witt vectors, and solved by a series corresponding to the automaton in Table 1 with 9 states.

Remark 5.1.4. If τ is an element of order 4 with break sequence $(1,3)$, then $\tau^{\circ 2}$ has break sequence (3), and hence is conjugate to the Klopsch's series $\sigma_{\mathrm{K},3}$ (see Example 1.3.1). Taking $\tau = \sigma_{\mathrm{CS}}$ produces the power series $\sigma := \sigma_{\mathrm{CS}}^{\circ 2} = t + t^4 + O(t^5)$, which satisfies $(t^2+1)X^2 + X + t^2 + t = 0$. The corresponding automaton is presented in Fig. 4, leading to the following explicit formula for an element of order 2 with break sequence (3):

$$\sigma_{\mathrm{CS}}^{\circ 2} = t + \sum_{k \geqslant 0} \sum_{\ell=0}^{2^k-1} t^{4\cdot 2^k + 2\ell} = t + \frac{1}{t^2+1} \sum_{k \geqslant 1} (t^{2\cdot 2^k} + t^{3\cdot 2^k}).$$

5.2. Order 4, break sequence $(1,5) = \langle 1,3 \rangle$

By Lubin's result ([53], [41, Thm. 2.2]), there is a unique conjugacy class of such power series. No formula for such a series is known, but following our philosophy, we can represent the solution by an automaton.

Proposition 5.2.1. *Up to conjugation, every element in $\mathscr{N}(\mathbf{F}_2)$ of order 4 with break sequence $(1,5) = \langle 1,3\rangle$ is given by the power series $\sigma_{(1,5)}$ corresponding to the automaton in Fig. 5 with 13 states, with initial coefficients*

$$\sigma_{(1,5)} = t + t^2 + t^3 + t^4 + t^6 + O(t^7).$$

Proof. Suitable algebraic equations are found from Witt's theory using Example 2.2.2; following Example 2.4.3, we start with the element $\beta := (z^{-1}, z^{-3}) \in W_2(\mathbf{F}_2(\!(z)\!))$, and rewrite the resulting equation in terms of the variables $x := \alpha_0$ and $y := \alpha_1 + \alpha_0^3 + \alpha_0^2$ as

$$\begin{cases} x^2 + x = z^{-1}; \\ y^2 + y = x^5 + x^3. \end{cases} \tag{18}$$

(The variable y is used instead of α_1 since that choice allows us to use Lemma 2.3.1.) Writing $z_0 = z, z_1, z_2$ for uniformisers of the fields in the tower of extensions

$$K_0 := \mathbf{F}_2(\!(z)\!) \subsetneq K_1 = K_0(x) = \mathbf{F}_2(\!(z_1)\!) \subsetneq K_2 = K_1(y) = \mathbf{F}_2(\!(z_2)\!),$$

we have $v_{z_1}(x) = v_{z_0}(z^{-1}) = -1$, so $v_{z_1}(x^5 + x^3) = -5$, and hence $v_{z_2}(y) = -5$ and $v_{z_2}(x) = -2$. Hence the extensions are all totally ramified and we can choose $t = x^2y^{-1}$ as uniformiser for K_2 (since $v_{z_2}(t) = 1$). A generator σ for the Galois group of K_2/K_0 is determined by

$$\begin{cases} \sigma(x) = x + 1; \\ \sigma(y) = y + x^2 + 1, \end{cases}$$

and with $t = x^2y^{-1}$ we compute that $\sigma(t) = (x^2+1)/(y+x^2+1)$. By eliminating x and y from these last two equations and the two equations in (18), we find that $\sigma = \sigma(t)$ satisfies the following (irreducible) equation over $\mathbf{F}_2(t)$:

$$t^2X^3 + (t+1)^3X + t^3 + t = 0. \tag{19}$$

Considering the sum and product of the three solutions, we find that there is a unique solution with $\sigma = t + O(t^2)$. The corresponding automaton with initial coefficients $t + t^2 + t^3 + t^4 + t^6 + O(t^7)$ and Equation (19) produced by the algorithm is displayed in Fig. 5. □

5.3. Order 4, break sequence $(1,9) = \langle 1,5\rangle$

Again by Lubin's result in [53], there is a unique conjugacy class of such power series. A corresponding automaton is found as follows.

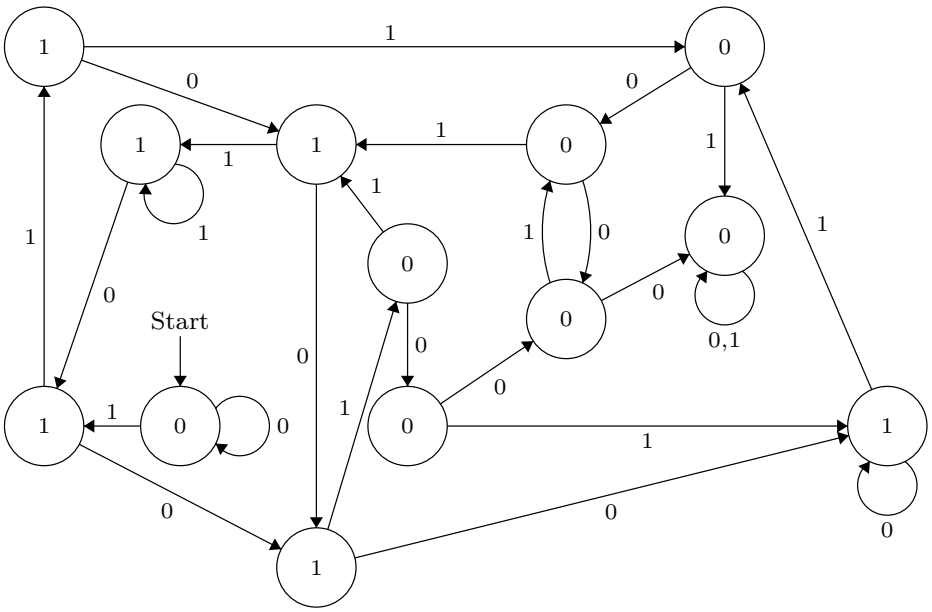


Fig. 5. Automaton representing a power series $\sigma_{(1,5)}$ of order 4 with break sequence $(1,5)$ (unique up to conjugation).

Proposition 5.3.1. *Up to conjugation, every element in $\mathscr{N}(\mathbf{F}_2)$ of order 4 with break sequence $(1,9) = \langle 1,5\rangle$ is given by the power series $\sigma_{(1,9)}$ corresponding to the automaton described as follows using the data in Table 2: it has 110 states, corresponding to the 110 triples on the displayed ordered list, where the start vertex is the first triple on the list and a triple (ℓ, i, j) occurs on the list precisely if the following three conditions hold: it has label ℓ, there is a directed edge with label 0 to the i-th triple on the list and there is a directed edge with label 1 to the j-th triple on the list. The initial coefficients of $\sigma_{(1,9)}$ are*

$$\sigma_{(1,9)} = t + t^2 + t^3 + t^4 + t^5 + t^6 + t^7 + t^9 + t^{11} + t^{12} + t^{13} + t^{17} + t^{18} + O(t^{19}).$$

Proof. Following Example 2.4.3(c), we start with $\beta = (z^{-1}, z^{-10}) \in W_2(\mathbf{F}_2(\!(z)\!))$. In the resulting equations $\wp(\alpha) = \beta$, change variables to $x := \alpha_0$ and $y := \alpha_1 + \alpha_0^{10} + \alpha_0^9 + \alpha_0^6 + \alpha_0^3 + \alpha_0$ to find

$$\begin{cases} x^2 + x = z^{-1}; \\ y^2 + y = x^9 + x. \end{cases}$$

Writing $z_0 = z$, z_1, z_2 for uniformisers of the fields in the tower of extensions

$$K_0 := \mathbf{F}_2(\!(z)\!) \subsetneq K_1 = K_0(x) = \mathbf{F}_2(\!(z_1)\!) \subsetneq K_2 = K_1(y) = \mathbf{F}_2(\!(z_2)\!),$$

we have $v_{z_1}(x) = -1$, so $v_{z_1}(x^9 + x) = -9$, and hence $v_{z_2}(y) = -9$, $v_{z_2}(x) = -2$ and $v_{z_2}(z) = 4$. Hence all extensions are totally ramified and we can choose $t = x^{-1}yz^2$ as uniformiser for K_2 (since $v_{z_2}(t) = 1$). A generator σ for the Galois group of K_2/K_0 is determined by

$$\begin{cases} \sigma(x) = x + 1; \\ \sigma(y) = y + x^4 + x^2 + x + 1. \end{cases}$$

By elimination of variables, we find that $\sigma = \sigma(t)$ satisfies the following (irreducible) equation over $\mathbf{F}_2(t)$:

$$t^2\sigma^7 + t^3\sigma^6 + (t^5 + t^4 + t^2)X^5 + (t^5 + t^3)X^4 + \\ (t^7 + t^5 + t^4 + t^3 + t)X^3 + t^5X^2 + (t^3 + t + 1)X + t = 0.$$

There is a unique solution of the form $t+O(t^2)$, and its initial coefficients are as indicated in the proposition; the corresponding 2-automaton can be found in Table 2 and in [17] (the visual representation in Table 2 is more of an illustration but can be manipulated directly in [17] using standard graph theory algorithms). □

6. Some new explicit formulas for power series of order 4

The explicit power series σ_{CS} and its inverse are a full set of representatives for the conjugacy classes of order-4 elements with break sequence $(1, 3)$. The series σ_{J} is another power series with a nice closed formula. We did a larger search for automata corresponding to such power series and found five more for which we could write down reasonably sized closed formulas. One of these is the inverse of Jean's series displayed in Equations (16), (17). We list the other four in Table 3.

We start with the equation from Example 2.3.2, but choose different uniformisers t. Recall that we write $\tau = \sigma^{\circ 3}$.

(i) First, let $t = (1 + x^2 + y)/(x^2 + xy)$. Then $\sigma = \sigma_{\mathrm{T},1}$ satisfies

$$t^2X^4 + (t^4 + t^2 + t + 1)X^2 + (t^3 + t^2 + t)X + t^3 = 0$$

and $\tau = \sigma_{\mathrm{T},2}$ satisfies

$$t^2X^4 + (t + 1)X^3 + (t^4 + t^2 + t)X^2 + (t^2 + t)X + t^2 = 0.$$

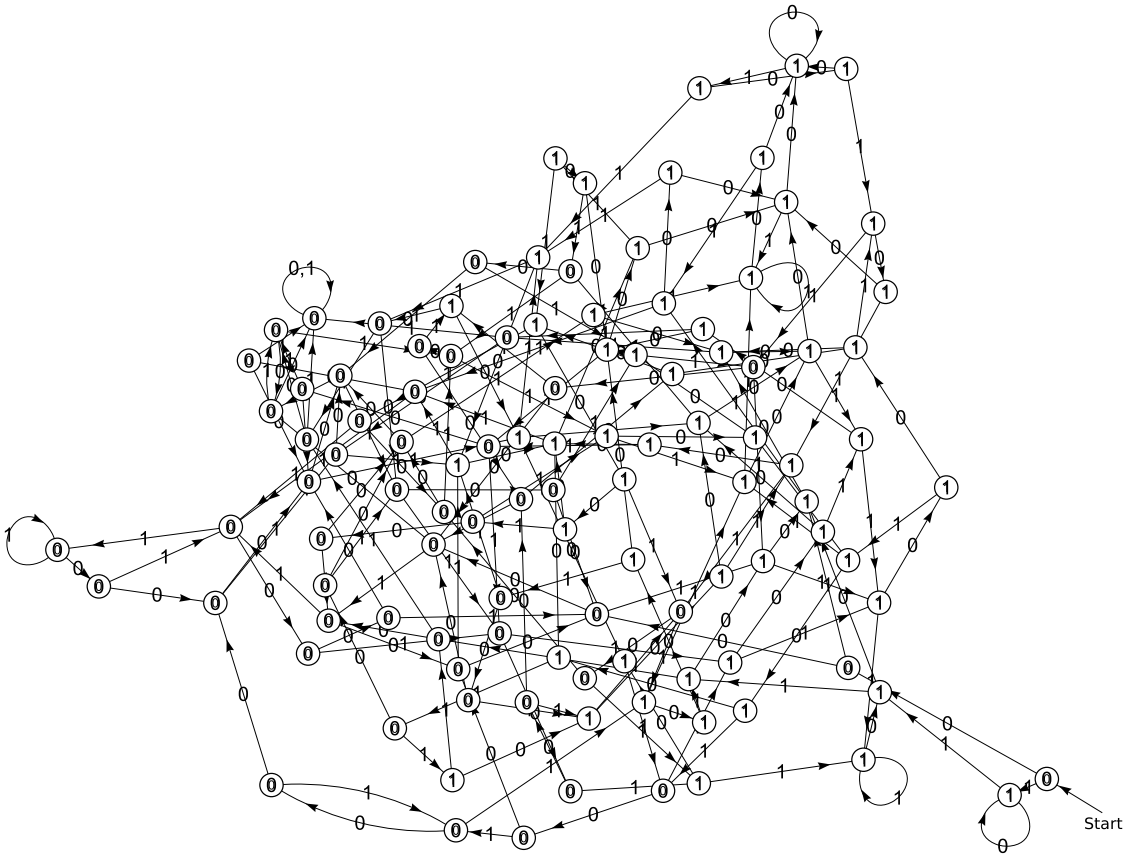
Solving these (irreducible) equations by automata, we find that $\sigma_{\mathrm{T},1}$ and $\sigma_{\mathrm{T},2}$ correspond to the top left, respectively top right automaton depicted in Table 4. It is relatively straightforward to convert the automata into explicit series following the method explained after Corollary 5.1.2, and the result is shown in Table 3 (including the initial coefficients).

(ii) Second, let $t = xy/(x^3 + y)$. Then $\sigma = \sigma_{\mathrm{T},3}$ satisfies

$$t^4X^4 + (t^2 + 1)X^3 + (t^3 + t)X^2 + t^2X + t^3 = 0$$

Table 2
Representation of the automaton for the power series $\sigma_{(1,9)}$ of order 4 with break sequence $(1, 9)$. The meaning of the representation by a set of triples is found in Proposition 5.3.1: a triple (ℓ, i, j) represents a vertex (the first one on the list being the start vertex) with vertex label ℓ, a directed edge with label 0 to the i-th triple, and with label 1 to the j-th triple.

$((0,2,3),(0,7,8),(1,3,69),(0,5,6),(0,12,13),(1,85,72),(0,20,16),(1,88,89),(0,10,11),(0,24,37),$
$(1,84,74),(0,24,40),(1,104,76),(0,15,16),(0,20,37),(1,8,72),(0,18,19),(0,30,13),(1,73,74),$
$(0,48,49),(0,22,23),(0,48,60),(1,91,92),(0,20,25),(1,81,94),(0,27,6),(0,35,28),(0,29,19),$
$(0,62,28),(0,31,9),(0,22,32),(1,88,78),(0,34,11),(0,31,49),(0,7,36),(1,105,52),(1,23,61),$
$(0,7,39),(1,106,14),(1,95,17),(0,42,36),(0,20,40),(0,22,36),(0,45,46),(0,31,60),(1,40,55),$
$(0,22,39),(0,50,51),(0,35,54),(0,50,50),(0,48,9),(0,53,54),(0,21,50),(0,59,57),(0,49,56),$
$(0,51,50),(0,58,57),(0,62,54),(0,66,4),(0,38,4),(0,60,56),(0,21,43),(0,30,54),(0,43,50),$
$(0,21,51),(0,21,7),(0,65,4),(0,47,9),(1,8,98),(1,70,71),(1,100,92),(1,75,76),(1,97,98),$
$(1,79,78),(1,81,82),(1,69,76),(1,70,78),(1,83,78),(1,77,80),(1,102,72),(1,88,90),(1,103,74),$
$(1,70,89),(1,39,82),(1,91,80),(1,77,87),(1,93,94),(1,79,64),(1,99,52),(1,101,14),(1,79,68),$
$(1,36,61),(1,106,68),(1,107,63),(1,91,96),(1,108,17),(1,106,41),(1,16,55),(1,77,92),(1,70,90),$
$(1,77,96),(1,106,64),(1,109,26),(1,23,26),(1,86,52),(1,86,67),(1,110,17),(1,105,67),(1,105,44),$
$(1,105,33))$



and $\tau = \sigma_{\mathrm{T},4}$ satisfies the same equation as σ (it turns out that another solution is $\sigma_{\mathrm{T},3}^{\circ 2} = \sigma_{\mathrm{T},4}^{\circ 2}$). Solving this (irreducible) equation by automata, we find that σ and τ correspond to the bottom left and bottom right automaton depicted in Table 4.

Table 3
Four explicit power series of order 4 with break sequence $(1,3)$ (the representation is minimal in the sense that no monomial occurs twice in the same formula).

$$\sigma_{\mathrm{T},1} = t + \sum_{k\geqslant 2}\left(t^{2^k-2} + t^{2\cdot 2^k-1} + t^{4\cdot 2^k-5}\right) + \sum_{k,\ell\geqslant 2} t^{2^k(2^\ell-3)+1} = t + t^2 + O(t^5).$$

$$\sigma_{\mathrm{T},2} = t + t^2 + \sum_{k\geqslant 3}\left(t^{2^k-4} + t^{2^k-3} + t^{2^k-1} + t^{4\cdot 2^k-6} + t^{4\cdot 2^k-5} + t^{8\cdot 2^k-22} + t^{8\cdot 2^k-21}\right) + (t+1)\sum_{k,\ell\geqslant 3} t^{2^k(2^\ell-6)+2} + (t+1)\sum_{k,\ell,m\geqslant 2} t^{2^{k+\ell}(2^m-3)+2\cdot 2^k-2} = t + t^2 + t^4 + t^5 + O(t^7).$$

$$\sigma_{\mathrm{T},3} = t + t^8 + t^{44} + \sum_{k\geqslant 2}\left(t^{2^k-2} + t^{3\cdot 2^k-2} + t^{8\cdot 2^k-4} + t^{8\cdot 2^k+4} + t^{8\cdot 2^k+20} + t^{16\cdot 2^k+44} + t^{24\cdot 2^k-4}\right) + \sum_{k,\ell\geqslant 2}\left(t^{2^k(2^\ell+3)-2} + t^{4\cdot 2^k(2^\ell+2)+4} + t^{8\cdot 2^k(2^\ell+3)-4} + t^{8\cdot 2^k(2^\ell+2)+12}\right) + \sum_{k,\ell\geqslant 2,m\geqslant 1}\left(t^{2^{k+\ell}(2^m+1)+2^k-2} + t^{8\cdot 2^{k+\ell}(2^m+1)+8\cdot 2^k-4}\right) = t + t^2 + t^6 + t^8 + t^{10} + O(t^{13}).$$

$$\sigma_{\mathrm{T},4} = t + t^4 + t^8 + t^{20} + \sum_{k\geqslant 2}\left(t^{2^k-2} + t^{8\cdot 2^k-4} + t^{8\cdot 2^k+20} + t^{16\cdot 2^k+12} + t^{16\cdot 2^k+44}\right) + \sum_{k,\ell\geqslant 2}\left(t^{2^k(2^\ell+1)-2} + t^{8\cdot 2^k(2^\ell+1)-4} + t^{4\cdot 2^k(2^\ell+2)+4} + t^{8\cdot 2^k(2^\ell+2)+12} + t^{2^k(2^\ell+3)-2} + t^{8\cdot 2^k(2^\ell+3)-4}\right) + \sum_{k,\ell\geqslant 2,m\geqslant 1}\left(t^{2^{k+\ell}(2^m+1)+2^k-2} + t^{8\cdot 2^{k+\ell}(2^m+1)+8\cdot 2^k-4}\right) = t + t^2 + t^4 + t^6 + t^8 + O(t^{13}).$$

Converting the automata into explicit series as before, we find the formulas in Table 3 (again including the initial coefficients).

By the criterion in Lemma 5.1.1, we see easily that $\sigma_{\mathrm{T},2}, \sigma_{\mathrm{T},3}$ and σ_{CS} are conjugate, and so are $\sigma_{\mathrm{T},1}, \sigma_{\mathrm{T},4}$ and $\sigma_{\mathrm{CS}}^{\circ 3}$.

7. Construction and classification of some order-8 elements

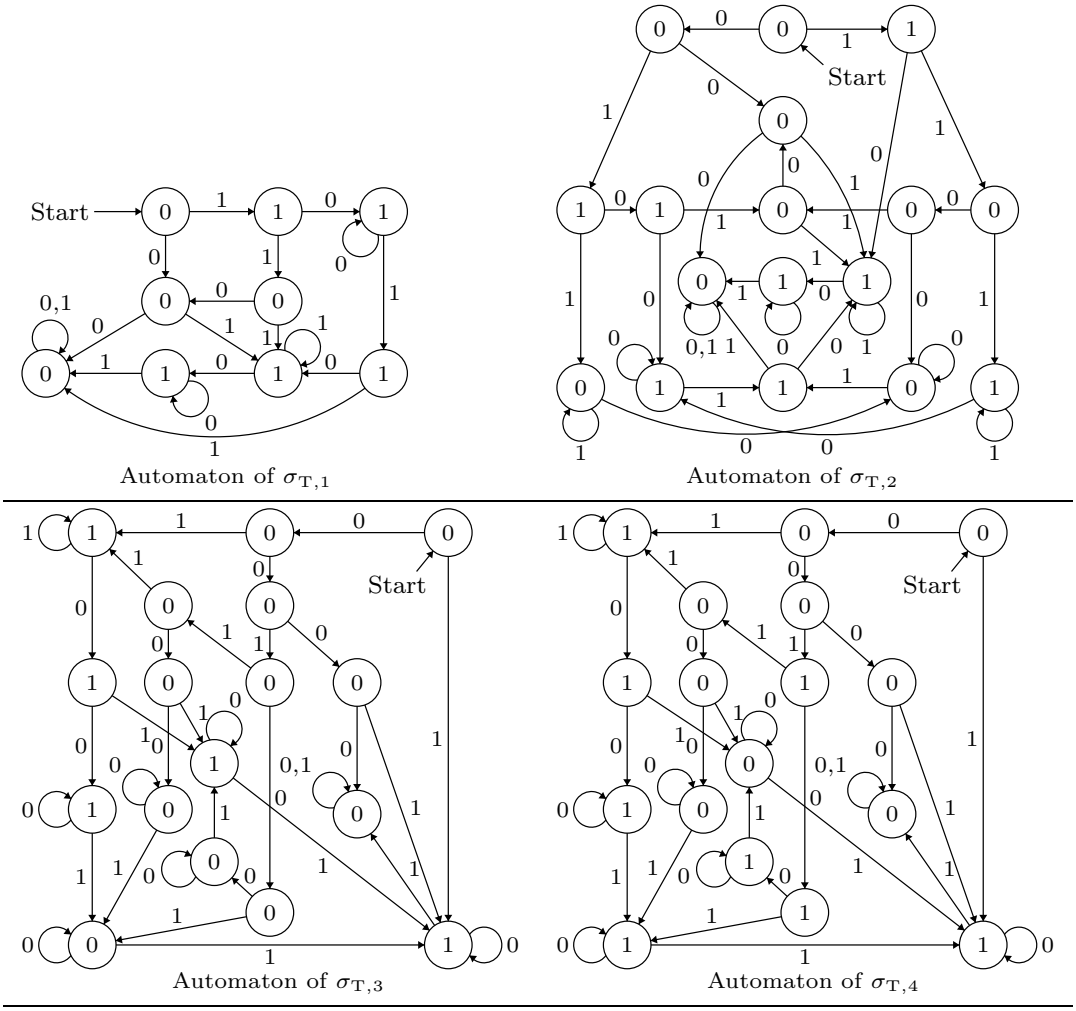
7.1. Order 8, break sequence $(1,3,11) = \langle 1,2,4\rangle$

Up to now, no finite description of any element of $\mathscr{N}(\mathbf{F}_2)$ of order 8 was known. Our method produces an example.

Proposition 7.1.1. *An element σ_8 in $\mathscr{N}(\mathbf{F}_2)$ of order 8 with break sequence $(1,3,11) = \langle 1,2,4\rangle$ is given by the automaton described by the data in Table 5: it has 320 states, corresponding to the 320 triples on the displayed ordered list, where the start vertex is the first triple on the list and a triple (ℓ,i,j) occurs on the list precisely if the following three conditions hold: its vertex label is ℓ, there is a directed edge with label 0 to the i-th triple on the list and there is a directed edge with label 1 to the j-th triple on the list. The initial terms of σ_8 are*

$$\sigma_8 = t + t^2 + t^5 + t^6 + t^{12} + O(t^{13}).$$

Table 4
Automata corresponding to the order 4, break sequence $(1, 3)$ series in Table 3.



We refrain from including a pictorial representation, but the automaton is stored in standard Mathematica form in [17], making it easy to manipulate.

Proof. We refer to Example 2.2.3 on how to use Witt vectors of length 3 to construct cyclic order-8 extensions. We choose $\beta = (z^{-1}, 0, 0) \in W_3(\mathbf{F}_2(\!(z)\!))$ and rewrite the resulting equations in (6) in terms of the variables $x := \alpha_0$, $y := \alpha_1$ and $w := \alpha_2 + \alpha_0^2\alpha_1$ to find

$$\begin{cases} x^2 + x = z^{-1}; \\ y^2 + y = xz^{-1}; \\ w^2 + w = x^4y + x^3y. \end{cases}$$

Choosing uniformisers $z_0 = z, z_1, z_2, z_3$ for the intermediate fields in the tower of field extensions

$$K_0 = \mathbf{F}_2(\!(z)\!) \subsetneq K_1 = K_0(x) = \mathbf{F}_2(\!(z_1)\!) \subsetneq K_2 = K_1(y) = \mathbf{F}_2(\!(z_2)\!) \subsetneq K_3 = K_2(w) = \mathbf{F}_2(\!(z_3)\!)$$

and using Lemma 2.3.1 as in Example 2.3.2, we see that the extension K_3/K_0 is totally ramified. We find the relevant valuations (following Lemma 2.3.1):

$$\begin{aligned} &v_{z_1}(x) = -1,\ v_{z_1}(z) = 2;\\ &v_{z_2}(y) = -3;\ v_{z_2}(x) = -2,\ v_{z_2}(z) = 4;\\ &v_{z_3}(w) = -11, v_{z_3}(x) = -4,\ v_{z_3}(y) = -6,\ v_{z_3}(z) = 8. \end{aligned}$$

We choose the uniformiser t as $t = (w+y)/(x^3+y)$. Then indeed $v_{z_3}(t) = 1$, and the action of the generator of the Galois group on α_i is given by (7), which implies that for our choice of variables we have

$$\begin{cases} \sigma(x) = x+1;\\ \sigma(y) = y+x;\\ \sigma(w) = w+xy+y, \end{cases} \tag{20}$$

and so by elimination we find the (irreducible) equation

$$t^6X^6 + (t^6+t^2)X^4 + (t^6+t^5+t^4+t^3+t^2+1)X^2 + (t+1)^3X + t^6+t^5+t^2+t = 0$$

for $\sigma = \sigma_8$. The initial coefficients are as indicated, and we readily verify the lower break sequence $(1,3,11)$ from

$$\sigma_8 = t + t^2 + O(t^3),\ \sigma_8^{\circ 2} = t + t^4 + O(t^5),\ \sigma_8^{\circ 4} = t + t^{12} + O(t^{13}). \quad \square$$

7.2. Detecting conjugacy using local class field theory

Proposition 7.2.1. *The number of conjugacy classes of elements of order* 8 *in* $\mathscr{N}(\mathbf{F}_2)$ *with 'minimal' break sequence* $(1,3,11) = \langle 1,2,4\rangle$ *is* 4.

Proof. We follow the method of Lubin [54]. For $k \geqslant 1$, write U_k for the multiplicative group of units $U_k = 1 + z^k\mathbf{F}_2[\![z]\!]$. By [54, Thm. 2.2] elements of exact order 2^n in $\mathscr{N}(\mathbf{F}_2)$ up to conjugation correspond bijectively to continuous surjective characters $\eta\colon U_1 \to \mathbf{Z}/2^n\mathbf{Z}$ up to so-called strict equivalence (the bijection arises from the restriction of the local reciprocity map to U_1). Strict equivalence of characters η and η' means that there exists $u \in \mathscr{N}(\mathbf{F}_2)$ with $\eta(u(z)/z) = 0$ and $\eta'(x) = \eta(x \circ u)$ for all $x \in U_1$. Moreover, the upper break sequence $\langle b^{(0)}, \dots, b^{(n-1)}\rangle$ can be read off from the corresponding character: $\eta(U_{b^{(i)}}) = 2^i\mathbf{Z}/2^n\mathbf{Z}$ and $\eta(U_{b^{(i)}+1}) = 2^{i+1}\mathbf{Z}/2^n\mathbf{Z}$ [54, Prop. 3.2].

In our case of order 8 elements with minimal break sequence, this implies that the corresponding characters factor through U_1/U_5 and map U_3 to $4\mathbf{Z}/8\mathbf{Z}$. Since we have an isomorphism of groups

$$\begin{aligned}\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} &\to U_1/U_5\\ (c,d) &\mapsto (1+z)^c(1+z^3)^d U_5,\end{aligned}$$

there are eight such characters $\eta_{a,b}$ determined by $\eta_{a,b}(1+z) = a \in (\mathbf{Z}/8\mathbf{Z})^*$ and $\eta_{a,b}(1+z^3) = 4b$ with $b \in \mathbf{Z}/2\mathbf{Z}$. We need to determine which of these are strictly equivalent. Write any $u \in \mathscr{N}(\mathbf{F}_2)$ in the form $u(z) = z(1+z)^\alpha(1+z^3)^\beta u_5$ with $\alpha \in \{0,\dots,7\}, \beta \in \{0,1\}$ and $u_5 \in U_5$. We have $\eta_{a,b}(u(z)/z) = a\alpha + 4b\beta \bmod 8$, and hence $\eta_{a,b}(u(z)/z) = 0$ if and only if $u(z) \equiv z \bmod z^6$ or $u(z) \equiv z + z^4 + bz^5 \bmod z^6$. Suppose then that

$$\eta_{a',b'}(x) = \eta_{a,b}(x \circ u), \tag{21}$$

and evaluate both sides for $x = 1+z$ and $x = 1+z^3$, respectively. For the first choice of u, we immediately find that $a' = a$ and $b' = b$. For the second choice of u, for $x = 1+z$, the left hand side of (21) evaluates to a' and the right hand side to $\eta_{a,b}((1+z)^5 U_5) = 5a$. For $x = 1+z^3$, the left hand side is b' and the right hand side $\eta_{a,b}((1+z^3)U_5) = b$.

We conclude that the strict equivalence class of $\eta_{a,b}$ consists of $\eta_{a,b}$ and $\eta_{5a,b}$, and there are indeed four strict equivalence classes in total. □

We state below an analogue of Lemma 5.1.1 that allows us to distinguish between these four conjugacy classes based on the first few coefficients of the power series.

Proposition 7.2.2. *Let $\sigma \in \mathscr{N}(\mathbf{F}_2)$ be an automorphism of order 8 with break sequence given by $(1,3,11) = \langle 1,2,4\rangle$, and write $\sigma = \sum_{i=1}^{\infty} a_i t^i$ with $a_i \in \mathbf{F}_2$. Then $a_1 = a_2 = 1$, $a_3 = 0$, $a_5 \neq a_7$, and σ is conjugate to a series $\sigma_{8,(b_4,b_{11})}$ of order 8 that has initial coefficients*

$$\sigma_{8,(b_4,b_{11})} = t + t^2 + b_4 t^4 + t^7 + b_{11} t^{11} + O(t^{12})$$

for a unique choice of $b_4, b_{11} \in \mathbf{F}_2$. In particular, the conjugacy class of σ depends only on $\sigma \bmod t^{12}$.

The series σ_8 is conjugate to $\sigma_{8,(1,1)}$ and $\sigma_8^{\circ 3}$ is conjugate to $\sigma_{8,(0,1)}$. These give representatives of two of the four conjugacy classes of minimally ramified series of order 8.

Proof. We will show that any such σ is conjugate to some $\sigma_{8,(b_4,b_{11})}$ modulo t^{12}, and that the series $\sigma_{8,(b_4,b_{11})}$ are not conjugate modulo t^{12} for the four different choices of (b_4,b_{11}). Since we know that there are 4 conjugacy classes of series σ satisfying the required assumptions, this shows that actual series $\sigma_{8,(b_4,b_{11})}$ of order 8 with minimal break sequence do exist.

We first note that $d(\sigma) = 1$ implies $a_1 = a_2 = 1$; computing $\sigma^{\circ 2}$, we get $\sigma^{\circ 2} = t + (1+a_3)t^4 + O(t^5)$, and $d(\sigma^{\circ 2}) = 3$ gives $a_3 = 0$; finally, $\sigma^{\circ 4} = t + (a_5 + a_7)t^{12} + O(t^{13})$, and since $d(\sigma^{\circ 4}) = 11$, we get $a_5 \neq a_7$.

Table 5
Representation of the automaton for the power series σ_8 of order 8 with break sequence $(1, 3, 11)$. The meaning of the representation by a set of triples is found in Proposition 7.1.1: a triple (ℓ, i, j) represents a vertex (the first one on the list being the start vertex) with vertex label ℓ, a directed edge with label 0 to the i-th triple, and with label 1 to the j-th triple.

$((0,2,3),(0,58,59),(1,82,185),(0,5,3),(0,65,66),(0,7,8),(0,136,137),(1,278,43),(0,10,11),(0,140,141),$
$(1,281,43),(0,13,8),(0,147,38),(0,15,11),(0,151,152),(0,17,18),(0,76,77),(1,279,117),(0,20,18),$
$(0,78,79),(0,22,23),(0,60,61),(1,280,117),(0,25,23),(0,70,72),(0,9,27),(1,89,190),(0,24,27),(0,30,31),$
$(0,44,41),(1,87,190),(0,32,31),(0,32,34),(1,72,189),(0,33,36),(1,224,160),(0,33,38),(1,214,154),$
$(0,40,41),(0,51,109),(1,84,185),(0,43,3),(0,115,116),(0,96,101),(0,46,3),(0,80,68),(0,35,48),$
$(1,272,112),(0,37,50),(1,290,45),(0,35,8),(0,37,53),(1,282,39),(0,55,18),(0,99,100),(0,57,27),$
$(0,142,143),(0,60,93),(1,238,128),(0,60,106),(1,236,87),(0,63,64),(0,58,112),(1,265,48),(0,151,129),$
$(1,242,66),(0,65,68),(1,260,59),(0,70,71),(0,151,179),(1,293,305),(1,231,97),(0,74,75),(0,95,199),$
$(1,232,97),(0,51,26),(1,268,48),(0,44,192),(1,267,143),(0,81,82),(0,195,154),(1,256,143),(0,81,84),$
$(1,246,273),(0,86,87),(0,195,162),(1,273,34),(0,86,89),(1,149,220),(0,91,92),(0,47,12),(1,234,87),$
$(0,94,89),(0,111,107),(0,96,97),(0,125,123),(1,23,34),(0,99,79),(0,125,128),(1,251,273),(1,222,220),$
$(0,103,101),(0,52,114),(0,105,89),(0,85,89),(0,4,107),(1,3,221),(0,54,109),(1,221,221),(0,56,107),$
$(0,129,130),(0,113,114),(0,138,139),(1,262,303),(0,131,132),(1,266,303),(0,118,116),(0,148,149),$
$(0,120,114),(0,150,50),(0,62,68),(0,73,123),(1,264,59),(0,90,123),(0,126,127),(0,126,75),(1,296,305),$
$(1,240,66),(0,153,28),(1,71,189),(0,153,42),(1,215,154),(0,131,134),(1,225,160),(0,129,27),(0,55,164),$
$(1,213,156),(0,98,172),(1,288,42),(0,63,16),(1,291,45),(0,63,6),(1,270,112),(0,140,145),(1,283,39),$
$(0,142,11),(0,52,122),(0,193,187),(1,212,156),(0,49,104),(0,148,194),(1,289,42),(0,58,124),(0,155,121),$
$(0,95,203),(0,157,121),(0,33,206),(0,159,46),(0,69,179),(0,161,46),(0,144,182),(0,163,122),(0,47,19),$
$(0,165,122),(0,99,21),(0,167,124),(0,133,106),(0,169,124),(0,83,40),(0,171,26),(0,176,29),(0,173,28),$
$(0,65,46),(0,175,26),(0,184,26),(0,44,189),(0,178,32),(0,142,168),(0,86,32),(0,181,29),(0,210,192),$
$(0,183,29),(0,211,186),(0,51,45),(0,154,186),(0,191,192),(0,129,188),(0,194,192),(0,179,188),$
$(0,162,186),(0,198,164),(0,187,193),(0,193,193),(0,205,166),(0,148,191),(0,197,162),(0,67,194),$
$(0,98,177),(0,200,164),(0,37,180),(0,202,162),(0,146,208),(0,204,166),(0,126,108),(0,49,110),$
$(0,207,168),(0,135,16),(0,209,168),(0,88,24),(0,55,156),(0,52,119),(1,319,100),(1,294,313),$
$(1,310,71),(1,316,308),(1,212,164),(1,218,172),(1,319,79),(1,218,177),(1,68,187),(1,66,187),$
$(1,223,158),(1,318,36),(1,311,145),(1,304,284),(1,227,203),(1,297,97),(1,227,199),(1,230,192),$
$(1,297,101),(1,230,189),(1,233,190),(1,233,31),(1,235,154),(1,244,72),(1,237,160),(1,241,141),$
$(1,239,196),(1,271,122),(1,241,170),(1,257,16),(1,243,129),(1,248,194),(1,243,179),(1,246,162),$
$(1,248,191),(1,246,154),(1,249,187),(1,249,193),(1,216,199),(1,252,201),(1,258,42),(1,217,172),$
$(1,255,174),(1,277,104),(1,257,6),(1,260,112),(1,260,124),(1,258,28),(1,261,93),(1,261,106),$
$(1,263,12),(1,292,26),(1,244,44),(1,228,102),(1,229,14),(1,247,9),(1,269,104),(1,294,12),(1,302,222),$
$(1,317,53),(1,312,134),(1,271,119),(1,275,119),(1,218,286),(1,277,110),(1,317,50),(1,309,84),$
$(1,277,306),(1,320,127),(1,315,314),(1,226,128),(1,295,303),(1,285,30),(1,245,87),(1,287,30),$
$(1,258,307),(1,249,221),(1,259,130),(1,276,48),(1,219,274),(1,223,8),(1,292,45),(1,223,48),$
$(1,294,19),(1,297,39),(1,280,123),(1,299,112),(1,252,132),(1,301,43),(1,247,82),(1,242,68),$
$(1,250,128),(1,244,71),(1,152,130),(1,298,307),(1,284,130),(1,300,307),(1,245,89),(1,247,84),$
$(1,241,145),(1,256,11),(1,253,274),(1,254,274),(1,259,27),(1,252,134),(1,318,38),(1,233,34),$
$(1,280,128),(1,320,75))$

We will now prove that σ is conjugate to $\sigma_{8,(b_4,b_{11})}$ for some $b_4, b_{11} \in \mathbf{F}_2$. We do this by conjugating with selected elements of $\mathscr{N}(\mathbf{F}_2)$ in the following steps (in each step the symbols a_i denote the coefficients of the 'new' power series, obtained by performing the conjugations described in the previous steps):

Step I (conjugating with $\chi_3 \colon t \mapsto t + t^3$). We have $\chi_3^{\circ -1} = t + t^3 + t^5 + t^9 + t^{11} + O(t^{12})$, yielding

$$\chi_3 \circ \sigma \circ \chi_3^{\circ -1} = t + t^2 + (1 + a_4)t^4 + (1 + a_5)t^5 + O(t^6),$$

so conjugating if necessary by χ_3 we may and do assume that $a_5 = 0$; then $a_7 = 1$, since $a_5 \neq a_7$.

Step II (conjugating with $\chi_5 \colon t \mapsto t+t^5$). We have $\chi_5^{\circ -1} = t+t^5+t^9+O(t^{12})$, yielding

$$\chi_5 \circ \sigma \circ \chi_5^{\circ -1} = t + t^2 + a_4 t^4 + (1+a_6)t^6 + O(t^7),$$

so conjugating if necessary by χ_5 we may and do assume that $a_6 = 0$.

Step III (conjugating with $\chi_2 \colon t \mapsto t + t^2$). We have $\chi_2^{\circ -1} = t + t^2 + t^4 + t^8 + O(t^{12})$, yielding

$$\chi_2 \circ \sigma \circ \chi_2^{\circ -1} = t+t^2+a_4 t^4+t^7+(1+a_8)t^8+(1+a_9)t^9+(a_9+a_{10})t^{10}+(1+a_{11})t^{11}+O(t^{12}),$$

so conjugating if necessary by χ_2 we may and do assume that $a_9 = 0$.

Step IV (conjugating with $\chi_6 \colon t \mapsto t + t^6$). We have $\chi_6^{\circ -1} = t + t^6 + O(t^{12})$, yielding

$$\chi_6 \circ \sigma \circ \chi_6^{\circ -1} = t + t^2 + a_4 t^4 + t^7 + (1+a_8)t^8 + (1+a_{10})t^{10} + a_{11}t^{11} + O(t^{12}),$$

so conjugating if necessary by χ_6 we may and do assume that $a_8 = 0$.

Step V (conjugating with $\chi_4 \colon t \mapsto t + t^4$). We have $\chi_4^{\circ -1} = t + t^4 + O(t^{12})$, yielding

$$\chi_4 \circ \sigma \circ \chi_4^{\circ -1} = t + t^2 + a_4 t^4 + t^7 + (1+a_{10})t^{10} + a_{11}t^{11} + O(t^{12}),$$

so conjugating if necessary by χ_4 we may and do assume that $a_{10} = 0$.

This ends the proof that σ is conjugate to $\sigma_{8,(b_4,b_{11})}$ for some $b_4, b_{11} \in \mathbf{F}_2$.

We will now prove that the power series $\sigma_{8,(b_4,b_{11})}$ and $\sigma_{8,(c_4,c_{11})}$ are not conjugate in $\mathscr{N}(\mathbf{F}_2)$ unless $(b_4, b_{11}) = (c_4, c_{11})$. Indeed, suppose that $\sigma_{8,(b_4,b_{11})}$ and $\sigma_{8,(c_4,c_{11})}$ are conjugate, and let $\tau \in \mathscr{N}(\mathbf{F}_2)$ be a conjugating power series, so that $\sigma_{8,(b_4,b_{11})} \circ \tau = \tau \circ \sigma_{8,(c_4,c_{11})}$. Write $\tau = t + \sum_{i=2}^{\infty} d_i t^i$. Computing $\sigma_{8,(b_4,b_{11})} \circ \tau - \tau \circ \sigma_{8,(c_4,c_{11})}$, we get

$$\begin{aligned}
&\sigma_{8,(b_4,b_{11})} \circ \tau - \tau \circ \sigma_{8,(c_4,c_{11})} \\
&= (d_3 + b_4 + c_4)t^4 + d_3 t^5 + (d_5 + d_3 c_4)t^6 + \\
&\quad (d_2 + d_6 + d_7 + d_2 b_4 + d_2 c_4 + d_3 c_4 + d_5 c_4)t^8 + (d_2 + d_5 + d_7 + d_3 c_4)t^9 + \\
&\quad (d_2 + d_4 + d_6 + d_7 + d_9 + d_3 c_4 + d_7 c_4)t^{10} + (d_2 + d_2 d_3 + d_7 + b_{11} + c_{11})t^{11} + O(t^{12}).
\end{aligned}$$

Considering the coefficients at t^5, t^6 and t^9 gives $d_3 = d_5 = d_2 + d_7 = 0$; looking then at the coefficients at t^4 and t^{11} gives $b_4 = c_4$ and $b_{11} = c_{11}$.

Applying the algorithm from the above proof, we find that σ_8 is conjugate to $\sigma_{8,(1,1)}$ and $\sigma_8^{\circ 3}$ is conjugate to $\sigma_{8,(0,1)}$. (This requires computing more coefficients than we have specified in Steps I and II, but the computations are easy.) □

Corollary 7.2.3. *Let $\sigma \in \mathscr{N}(\mathbf{F}_2)$ be an automorphism of order 8 with break sequence $(1,3,11) = \langle 1,2,4 \rangle$. Then σ and $\sigma^{\circ 5}$ are conjugate in $\mathscr{N}(\mathbf{F}_2)$, while σ and $\sigma^{\circ 3}$ are not.*

Proof. This follows from the proof of Proposition 7.2.1—if an element σ corresponds to the character $\eta_{a,b}$, then for k odd the element $\sigma^{\circ k}$ corresponds to $k\eta_{a,b} = \eta_{ka,kb} = \eta_{ka,b}$. Since $\eta_{a,b}$ and $\eta_{5a,b}$ are strictly equivalent, while $\eta_{a,b}$ and $\eta_{3a,b}$ are not, the claim follows.

It is also possible to give a direct proof using the method of Proposition 7.2.2, as follows. Denote the relation of being conjugate by $\sim$. By Proposition 7.2.2, we may assume without loss of generality that $\sigma = t + t^2 + b_4t^4 + t^7 + b_{11}t^{11} + O(t^{12})$ for some $b_4, b_{11} \in \mathbf{F}_2$. Then

$$\sigma^{\circ 2} = t + t^4 + t^8 + t^9 + (1 + b_4)t^{10} + t^{11} + O(t^{12}), \qquad \sigma^{\circ 4} = t + O(t^{12}),$$

and hence $\sigma = \sigma^{\circ 5} + O(t^{12})$ and

$$\sigma^{\circ 3} = t + t^2 + (1 + b_4)t^4 + t^7 + t^9 + b_4t^{10} + (1 + b_{11})t^{11} + O(t^{12}).$$

Following the algorithm of the proof of Proposition 7.2.2 (and using the notation therein), we may conjugate $\sigma^{\circ 3}$ in turn by χ_2, χ_6 and in the case where $b_4 = 1$ also χ_4 to arrive at

$$\sigma^{\circ 3} \sim t + t^2 + (1 + b_4)t^4 + t^7 + b_{11}t^{11} + O(t^{12}),$$

i.e. if $\sigma \sim \sigma_{8,(b_4,b_{11})}$, then $\sigma^{\circ 3} \sim \sigma_{8,(b_4+1,b_{11})}$. Applying Proposition 7.2.2 again shows that $\sigma \sim \sigma^{\circ 5}$ and $\sigma \nsim \sigma^{\circ 3}$. □

7.3. Finding representatives via explicit class field theory

We have already constructed representatives of two out of four conjugacy classes of minimally ramified series of order 8. In order to construct the representatives for the remaining conjugacy classes, we will extend the method using the Carlitz module from Remark 5.1.3.

Let ρ be the Carlitz module for $K = \mathbf{F}_2(z)$. We know from [54, Obs. 4 & Sect. 5] that the characters $\eta\colon U_1 \to \mathbf{Z}/8\mathbf{Z}$ corresponding to minimally ramified order-8 elements factor through U_5, and the corresponding Galois extensions can be obtained as a subextension of $K(\rho[z^5])/K$. The extension $K(\rho[z^5])/K$ has Galois group

$$G = \left(\mathbf{F}_2[z]/z^5\right)^* \cong \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} = \langle z + 1 \bmod z^5\rangle \times \langle z^3 + 1 \bmod z^5\rangle.$$

The group G has two subgroups with quotient $\mathbf{Z}/8\mathbf{Z}$:

$$H_1 = \langle z^3 + 1 \bmod z^5\rangle \qquad \text{and} \qquad H_2 = \langle z^4 + z^3 + 1 \bmod z^5\rangle.$$

The field $K(\rho[z^5])$ is generated by a root α of the degree-16 polynomial $\rho_{z^5}(X)/\rho_{z^4}(X)$. The fixed fields L_1 and L_2 of H_1 and H_2, respectively, are generated by the elements

$$\beta_1 := \alpha \cdot \rho_{z^3+1}(\alpha) \qquad \text{and} \qquad \beta_2 := \alpha \cdot \rho_{z^4+z^3+1}(\alpha).$$

Recalling that L_i/K has Galois group cyclic of order 8 generated by σ acting as $\sigma(\alpha) = z\alpha + \alpha + \alpha^2$, we can compute $\sigma(\beta_i)$ and we find that

$$\begin{cases} \beta_1 = \alpha^9 + (z^4+z^2+z)\alpha^5 + (z^4+z^3+z^2)\alpha^3 + (z^3+1)\alpha^2; \\ \sigma(\beta_1) = \alpha^{10} + (z+1)\alpha^9 + (z^4+z^2+z)\alpha^6 + (z^5+z^4+z^3+z)\alpha^5 + \\ \qquad (z^4+z^3+z^2+1)\alpha^4 + (z^5+z^3+z^2)\alpha^3 + (z^4+z^3+z^2+z+1)\alpha^2 + \\ \qquad (z^2+z)\alpha; \end{cases}$$

and

$$\begin{cases} \beta_2 = \alpha^9 + (z^4+z^2+z)\alpha^5 + (z^4+z^3+z^2)\alpha^3 + (z^3+1)\alpha^2 + z\alpha; \\ \sigma(\beta_2) = \alpha^{10} + (z+1)\alpha^9 + (z^4+z^2+z)\alpha^6 + (z^5+z^4+z^3+z)\alpha^5 + \\ \qquad (z^4+z^3+z^2+1)\alpha^4 + (z^5+z^3+z^2)\alpha^3 + (z^4+z^3+z^2+z+1)\alpha^2 + \\ \qquad (z^2+z)\alpha. \end{cases}$$

Since z is the only ramified place and it is totally ramified in $K(\rho[z^5])$, the same is true in L_i. We can choose $t = \beta_i$ as a uniformiser for the place above z in L_i. Elimination of z and α leads to the following equation for the element $\sigma_{8,1} = \sigma_{8,1}(t)$ of order 8 with $t = \beta_1$:

$$tX^6 + (t+1)X^5 + \left(t^5+t^3+t\right)X^4 + \left(t^5+t^2+t\right)X^3 + \left(t^6+t^3+t\right)X^2 + t^4X + t^6 + t^5 + t^4 + t^3 = 0;$$

and to the following equation for the element $\sigma_{8,2} = \sigma_{8,2}(t)$ of order 8 with $t = \beta_2$:

$$tX^6 + (t+1)X^5 + \left(t^5+t^3\right)X^4 + \left(t^5+t+1\right)X^3 + \left(t^6+t^5+t^4+t^3+t\right)X^2 + \left(t^4+t^2\right)X + t^4 + t^3 = 0.$$

These equations define algebraic curves of geometric genus 7, solved by the series

$$\sigma_{8,1}(t) = t + t^2 + t^5 + t^{11} + O(t^{13}) \qquad \text{and} \qquad \sigma_{8,2}(t) = t + t^2 + t^5 + t^9 + t^{11} + O(t^{13})$$

of order 8, which are produced by automata with 668 and 926 states, respectively. Furthermore, $\sigma_{8,1}$ is conjugate to $\sigma_{8,(1,1)}$ and $\sigma_{8,2}$ is conjugate to $\sigma_{8,(1,0)}$ by the method from Proposition 7.2.2. We may summarise the above discussion as follows:

Proposition 7.3.1. *There are four conjugacy classes of order-8 elements with break sequence* $(1,3,11) = \langle 1,2,4\rangle$ *and their representatives are the series* $\sigma_{8,1}$, $\sigma_{8,1}^{\circ 3}$ (*conjugate to* σ_8 *and* $\sigma_8^{\circ 3}$, *respectively*), $\sigma_{8,2}$ *and* $\sigma_{8,2}^{\circ 3}$. □

The automata and series, also for $\sigma_{8,2}$, may be found in [17].

Remark 7.3.2. We have constructed order-8 elements by using the Galois extension $K(\rho[z^5])/K$ with Galois group $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, and looking at its subextensions L_i/K with Galois group $\mathbf{Z}/8\mathbf{Z}$. We could instead look at an extension $K(\rho[z^5])/M$ with Galois group $\mathbf{Z}/8\mathbf{Z}$. This would work, but would produce a non-minimally ramified series generated by an automaton with many more states—the automaton corresponding to $\sigma(t) = \rho_{1+z}(t)$ with $t = \alpha$ has 136600 states.

8. Embedding the Klein four-group in $\mathscr{N}(\mathbf{F_2})$ using automata

Since every p-group embeds in $\mathscr{N}(\mathbf{F}_p)$, we may ask for a representation for generators of a given p-group through automata. We show how to do this for the easiest case, that of the Klein four-group $V = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ for $p = 2$, by describing two automata that correspond to two commuting power series of order two in characteristic two (with minimal admissible break sequences), answering a question that Klopsch asked us.

8.1. Embedding with small conductor

For a general field $\mathbf{F}$, define the Nottingham group $\mathscr{N}(\mathbf{F})$ to be the group of power series $\sigma(t) \in \mathbf{F}[\![t]\!]$ of the form $t + O(t^2)$ under composition. The following lemma shows that it is easy to embed V into the Nottingham group over any proper field extension $\mathbf{F}$ of $\mathbf{F}_2$ such that all nontrivial elements of V have break sequence (1) (i.e. have depth 1), but one cannot do so over $\mathbf{F}_2$.

Proposition 8.1.1. *There is an embedding of the Klein four-group $V = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ in the Nottingham group $\mathscr{N}(\mathbf{F})$ over a field $\mathbf{F}$ of characteristic two with all nontrivial elements of V having break sequence* (1) *if and only if $\mathbf{F} \neq \mathbf{F}_2$.*

Note that all nontrivial elements having break sequence (1) means that the corresponding V-extension is *weakly ramified*, i.e. has trivial second ramification group. A much more general statement that implies Lemma 8.1.1 is given in [29, Korollar 3.2], but we give a short direct proof.

Proof. Assume $\mathbf{F} \neq \mathbf{F}_2$ and let U be a two-dimensional $\mathbf{F}_2$-vector subspace of $\mathbf{F}$. Then the power series $t/(ut+1) = t + ut^2 + O(t^3)$ taken over $u \in U$ form a subgroup of $\mathscr{N}(\mathbf{F})$ isomorphic to the Klein four-group.

For the converse, assume we have an embedding of $V = \{\mathrm{id}, \sigma, \tau, \sigma \circ \tau\}$ into $\mathscr{N}(\mathbf{F}_2)$ with nontrivial elements having break sequence (1). Then σ and τ are of the form $t + t^2 + O(t^3)$, implying that $\sigma \circ \tau = t + O(t^3)$, a contradiction. □

There are further restrictions on possible depths of elements of the Klein four-group embedded in $\mathscr{N}(\mathbf{F}_2)$. In the next subsection, we will construct an embedding with non-

trivial elements having depths $1, 1$ and 5. The next lemma shows that these are the minimal possible values.

Proposition 8.1.2. *For every embedding of the Klein four-group V in the Nottingham group $\mathscr{N}(\mathbf{F}_2)$ some nontrivial element of V has depth at least 5.*

Proof. Suppose the contrary. By Proposition 8.1.1 some nontrivial element has depth at least 2. Every element of finite order has odd depth: if σ had even depth, writing $\sigma = t + t^k + O(t^{k+1})$ with k odd, we would find by induction that $\sigma^{\circ 2^n} = t + t^{2^n(k-1)+1} + O(t^{2^n(k-1)+2})$ for all $n \geqslant 1$, so σ would not be of finite order. Also note that for every $k \geqslant 1$ the elements of depth at least k form a subgroup. Thus, the only possible sequences of depths < 5 of series in $\mathscr{N}(\mathbf{F}_2)$ representing nontrivial elements of V are $1, 1, 3$ and $3, 3, 3$. The latter is impossible, since the product of two elements of depth k has depth at least $k + 1$.

It remains to treat the case where the depths of the nontrivial elements are $1, 1, 3$. By Klopsch's theorem [48] every element of order 2 and depth 1 is conjugate to $t/(t+1)$, so without loss of generality we may assume that $V = \{\mathrm{id}, \sigma, \tau, \sigma \circ \tau\}$ with

$$\sigma(t) = \frac{t}{t+1} \qquad \text{and} \qquad \tau(t) = t + t^2 + \sum_{i \geqslant 3} a_i t^i.$$

We will reach a contradiction by computing up to order $O(t^9)$. We have

$$\begin{aligned}\tau^{\circ 2}(t) = t + (1 + a_3)t^4 + (a_3 a_4 + a_5)t^6 + \\ (a_3 + a_3 a_4 + a_4 a_5 + a_6 + a_3 a_6 + a_7)t^8 + O(t^9).\end{aligned}$$

Since $\tau^{\circ 2} = \mathrm{id}$, this gives $a_3 = 1$, $a_4 = a_5$, and $a_7 = 1$. Substituting these values allows us to compute

$$\begin{aligned}(\sigma \circ \tau)(t) = t + (1 + a_4)t^4 + (1 + a_4)t^5 + (a_4 + a_6)t^6 + (1 + a_4)t^7 + \\ (1 + a_4 + a_6 + a_8)t^8 + O(t^9); \\ (\tau \circ \sigma)(t) = t + (1 + a_4)t^4 + (1 + a_4)t^5 + (a_4 + a_6)t^6 + (1 + a_4)t^7 + \\ (a_6 + a_8)t^8 + O(t^9).\end{aligned}$$

Since $\sigma \circ \tau = \tau \circ \sigma$, this gives $a_4 = 1$, and shows that the depth of $\sigma \circ \tau$ is at least 5. □

8.2. Using automata

We now show how to use automata to embed the Klein four-group V into $\mathscr{N}(\mathbf{F}_2)$. We start with the V-extension $\mathbf{F}_2(\!(z)\!)(x, y)$ of $\mathbf{F}_2(\!(z)\!)$ given by $x^2 + x = z^{-1}$ and $y^2 + y = z^{-3}$ with two generators $\sigma_{V,1}, \sigma_{V,2}$ of V acting as

$$\begin{cases} \sigma_{V,1}(x) = x+1; \\ \sigma_{V,1}(y) = y \end{cases} \quad \text{and} \quad \begin{cases} \sigma_{V,2}(x) = x; \\ \sigma_{V,2}(y) = y+1. \end{cases}$$

Since $\sigma_{V,1}, \sigma_{V,2}$ are different, of order two and commute, they generate the group V. Set $w = y + x^3 + x^2 + x$. We may regard $\mathbf{F}_2(\!(z)\!)(x,y)$ as the extension $\mathbf{F}_2(\!(z)\!)(x,y) = \mathbf{F}_2(\!(z)\!)(x,w)$ of $\mathbf{F}_2(\!(z)\!)$ given by

$$\begin{cases} x^2 + x = z^{-1}; \\ w^2 + w = x^5 + x \end{cases}$$

with the two generators $\sigma_{V,1}$ and $\sigma_{V,2}$ acting on x and w as

$$\begin{cases} \sigma_{V,1}(x) = x+1; \\ \sigma_{V,1}(w) = w + x^2 + x + 1 \end{cases} \quad \text{and} \quad \begin{cases} \sigma_{V,2}(x) = x; \\ \sigma_{V,2}(w) = w+1. \end{cases}$$

Writing $z_0 = z$, z_1, z_2 for uniformisers of the fields in the tower of field extensions

$$K_0 := \mathbf{F}_2(\!(z)\!) \subsetneq K_1 = K_0(x) = \mathbf{F}_2(\!(z_1)\!) \subsetneq K_2 = K_1(w) = \mathbf{F}_2(\!(z_2)\!),$$

we have $v_{z_1}(x) = -1$, $v_{z_1}(x^5 + x) = -5$, and hence $v_{z_2}(w) = -5$ and $v_{z_2}(x) = -2$. Choosing a uniformiser $t = x^2 w^{-1}$ (note that $v_{z_2}(t) = 1$), we find by elimination of the variables z, x, w that $\sigma_{V,1} = \sigma_{V,1}(t)$ and $\sigma_{V,2} = \sigma_{V,2}(t)$ satisfy, respectively,

$$t^4X^4 + t^3X^3 + X^2 + (t+1)X + t^2 + t = 0;$$
$$(t^4+1)X^4 + tX^2 + t^2X + t^4 = 0.$$

This is solved with respective initial coefficients

$$\sigma_{V,1} = t + t^2 + O(t^3) \qquad \text{and} \qquad \sigma_{V,2} = t + t^6 + O(t^7).$$

The corresponding automata have 18 and 14 states, respectively.

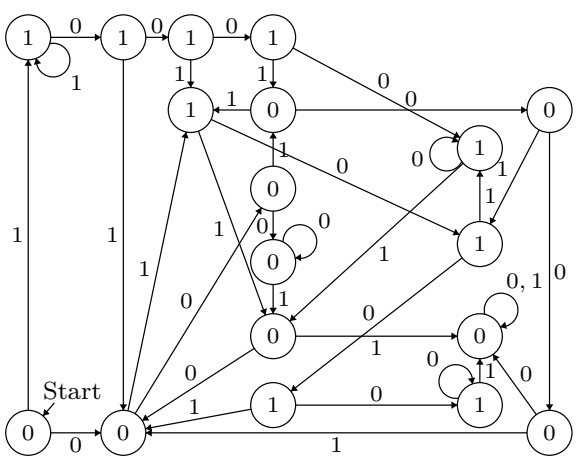
Proposition 8.2.1. *The series $\sigma_{V,1}$ and $\sigma_{V,2}$ have break sequences* (1) *and* (5) *and satisfy $\sigma_{V,1}^{\circ 2} = \sigma_{V,2}^{\circ 2} = t$ and $\sigma_{V,1} \circ \sigma_{V,2} = \sigma_{V,2} \circ \sigma_{V,1}$, and hence exhibit an explicit embedding of the Klein four-group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ into $\mathscr{N}(\mathbf{F}_2)$. The corresponding automata are depicted in Table 6.* □

For completeness, writing $\sigma_{V,3} = \sigma_{V,1} \circ \sigma_{V,2}$ for the third nontrivial element of V, we find that $\sigma_{V,3}$ satisfies

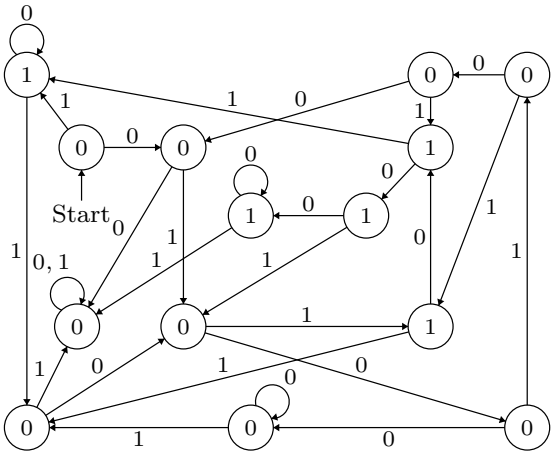
$$t^4X^4 + (t+1)^3X^3 + (t^3+t^2+t)X^2 + (t+1)^3X + t^3 + t = 0$$

with initial coefficients $\sigma_{V,3} = t + t^2 + t^3 + O(t^5)$, leading to an automaton with 25 states. The automaton is stored in standard Mathematica form in [17].

Table 6
Automata corresponding to the elements $\sigma_{V,1}$ and $\sigma_{V,2}$ that generate a copy of the Klein four-group in $\mathscr{N}(\mathbf{F}_2)$.



Automaton of $\sigma_{V,1}$



Automaton of $\sigma_{V,2}$

8.3. Other p-groups

In principle, since any finite p-group G can be realised explicitly as the Galois group of an extension of $\mathbf{F}_2(\!(z)\!)$ (this follows from Witt's work; see, e.g. the proof of [20, Theorem 3]), the Galois-theoretic method can be used to find equations satisfied by generators of an embedding of G into $\mathscr{N}(\mathbf{F}_p)$ by algebraic power series, and thus to represent them explicitly by automata. Recall from Remark 2.1.1 that any embedding of G into $\mathscr{N}(\mathbf{F}_p)$ can be conjugated into one in which the elements of G are represented by algebraic power series.

The examples in the current paper do not constitute the computational limit of the method. For example, we can give an embedding of $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ into $\mathscr{N}(\mathbf{F}_2)$ with two generators being produced by automata with 128 states, the order-4 element being minimally ramified and the order-2 element having depth 7; we can also obtain an order-9 element in $\mathscr{N}(\mathbf{F}_3)$ with break sequence $(1,7) = \langle 1,3\rangle$ produced by an automaton with 3634 states, etc. However, we refrain from further expanding the catalogue of examples.

As pointed out by the reviewer, it would be interesting to provide explicit automata representing embeddings of generators of other (non-commutative) finite 2-groups in $\mathscr{N}(\mathbf{F}_2)$ (or $\mathscr{N}(\mathbf{F}_{2^m})$ for general m), such as the dihedral or quaternion group of order 8; for this, one again needs to explicitly find a Galois realisation of such groups over $\mathbf{F}_{2^m}(\!(z)\!)$, e.g. by constructing a corresponding Katz–Gabber cover of $\mathbf{P}^1$. For the dihedral group, explicit realisations and a study of possible break sequences can be found in [65, §5, §4], at least for sufficiently large m. Also, the quaternion group Q acts by automorphisms (defined over $\mathbf{F}_4$) on the supersingular elliptic curve in characteristic 2 and stabilises the point at infinity. We did not pursue these lines of thought all the way up to an explicit automatic representation.

A challenge of a completely different level is to consider the question of embedding infinite groups in $\mathscr{N}(\mathbf{F}_p)$ using algebraic power series. Recall that Camina has proven that every countably based pro-p group embeds as subgroup in $\mathscr{N}(\mathbf{F}_p)$; thus, for example, the free pro-p group and the abstract free group on two generators embed. For the latter group, the question is whether we can find two algebraic (i.e. automatic) power series in $\mathscr{N}(\mathbf{F}_2)$ that generated a free group. Another example is the (first) Grigorchuk group, a 2-group with three generators, but without finite presentation (a countable set of relations was given by Lysënok); or other groups given by endomorphic presentations, see [6]. In all these cases, the Galois covering methods break down, and we do not know whether the Grigorchuk group may be realised inside $\mathscr{N}(\mathbf{F}_2)$ with all elements being described solely by algebraic (i.e. automatic) power series, i.e. whether the three generators can simultaneously be conjugated into a set of such algebraic power series (since it is residually finite, this property is true residually, but it is not clear how or whether the property lifts to the entire group).

9. State complexity of automata representing finite order elements in $\mathscr{N}(\mathbf{F}_p)$

9.1. General bounds on state complexity

How 'complex' is an automaton that computes a power series $\sigma \in \mathscr{N}(\mathbf{F}_p)$ of given order and break sequence? This is usually measured by 'state complexity', i.e. the minimal number of states in an automaton that computes the series.

This complexity can be bounded theoretically. The currently best results arise from the differential forms method described in Section 2: start with an algebraic equation (assumed irreducible) satisfied by $\sigma = \sigma(t)$ with coefficients from $\mathbf{F}_p[t]$, and consider it instead as a two-variable equation $F(t, X) = 0$ describing a (possibly singular) algebraic curve over $\mathbf{F}_p$. Consider the *degree*

$$d_\sigma := [\mathbf{F}_p(\sigma, t) : \mathbf{F}_p(t)] = \deg_X F$$

and the *height*

$$h_\sigma := [\mathbf{F}_p(\sigma, t) : \mathbf{F}_p(\sigma)] = \deg_t F$$

(the latter two equalities hold by the irreducibility of F), and let g_σ denote the genus of the normalisation $\mathscr{X}$ of the projective curve defined by $F(t, X) = 0$. Bridy has proven that the series σ can be realised by an automaton with less than

$$p^{h_\sigma + 3d_\sigma + g_\sigma - 1}$$

states (see [13, Cor. 3.10], a result that assumes, like this paper, the leading zeros convention, see [13, Remark 2.1]). Concerning the optimality of the upper bound, Bridy has shown in [13, Prop. 3.14] for every $h \geqslant 1$, there are power series with

Table 7
For each series, we give: its compositional order, lower break sequence, the degree d_σ and genus g_σ of the algebraic equation it satisfies, the theoretical interval $[\lfloor \log_2(d_\sigma+1)\rfloor, 2^{4d_\sigma+g_\sigma-1}]$ for the number of states of a minimal automaton and the actual number of states ('?' means we conjecture this to be the correct answer, '×' means we do not know the answer; see Remark 9.2.2).

series	order	breaks	$d_\sigma = h_\sigma$	g_σ	bounds	# of states
$\sigma_{\mathrm{S},1}$	2	(1)	2	1	$[1, 2^8]$	5
$\sigma_{\mathrm{S},m=2^\mu-1>1}$	2	$\frac{m+1}{2}$	$\frac{m-1}{2}$	$[\mu-1, 2^{\frac{5m+1}{2}}]$	$\mu+3$	
$\sigma_{\mathrm{S},m=2^\mu+1}$	2	$m-1$	$\frac{(m-1)(m-2)}{2}$	$[\mu, 2^{\frac{m^2+5m-8}{2}}]$	$2^\mu+3^\mu$?	
$\sigma_{\mathrm{K},3}$	2	(3)	3	1	$[2, 2^{12}]$	6
$\sigma_{\mathrm{K},m}$	2	(m)	m	$\frac{(m-1)(m-2)}{2}$	$[\lfloor \log_2(m+1)\rfloor, 2^{\frac{m(m+5)}{2}}]$	×
$\sigma_{\mathrm{CS}}^{\circ 2}$	2	(3)	2	1	$[1, 2^8]$	7
$\sigma_{V,1}$	2	(1)	4	2	$[2, 2^{17}]$	18
$\sigma_{V,2}$	2	(5)	4	2	$[2, 2^{17}]$	14
$\sigma_{V,3}$	2	(1)	4	2	$[2, 2^{17}]$	25
$\sigma_{\min}$	4	(1, 3)	3	1	$[2, 2^{12}]$	5
σ_{CS}	4	(1, 3)	2	1	$[1, 2^8]$	7
$\sigma_{\mathrm{CS}}^{\circ 3}$	4	(1, 3)	2	1	$[1, 2^8]$	7
σ_{J}	4	(1, 3)	2	1	$[1, 2^8]$	9
$\sigma_{\mathrm{J}}^{\circ 3}$	4	(1, 3)	2	1	$[1, 2^8]$	11
$\sigma_{\mathrm{T},1}$	4	(1, 3)	4	1	$[2, 2^{16}]$	9
$\sigma_{\mathrm{T},2}, \sigma_{\mathrm{T},3}, \sigma_{\mathrm{T},4}$	4	(1, 3)	4	1	$[2, 2^{16}]$	17
$\sigma_{(1,5)}$	4	(1, 5)	3	2	$[2, 2^{13}]$	13
$\sigma_{(1,9)}$	4	(1, 9)	7	4	$[3, 2^{31}]$	110
σ_8	8	(1, 3, 11)	6	7	$[2, 2^{30}]$	320

$d_\sigma = 1, h_\sigma = h, g_\sigma = 0$ that require at least $\geqslant p^h$ states. A lower bound for the minimal amount of states required to realise the given power series is given by $\log_p(d_\sigma+1)$ [13, Prop. 2.13]; this bound appears optimal when running over all algebraic power series ([13]).

9.2. Degree equals height for series of finite order in $\mathscr{N}(\mathbf{F}_p)$

In our situation we have the following extra information.

Proposition 9.2.1. *Let $\sigma(t) \in \mathbf{F}_p(\!(t)\!)$ be an algebraic power series over $\mathbf{F}_p(t)$ of finite compositional order. Then $d_\sigma = h_\sigma$.*

Proof. Write n for the compositional order of $\sigma(t)$. The map σ, regarded as an automorphism of $\mathbf{F}_p(\!(t)\!)$, restricts to an automorphism of the field

$$K := \mathbf{F}_p(t, \sigma(t), \sigma^{\circ 2}(t), \ldots, \sigma^{\circ(n-1)}(t)).$$

Since $\sigma(t)$ is algebraic over $\mathbf{F}_p(t)$, successive application of the automorphism σ shows that $\mathbf{F}_p(\sigma^{\circ k}(t))$ is algebraic over $\mathbf{F}_p(\sigma^{\circ(k-1)}(t))$ for $k \geqslant 1$, and hence the extension $K/\mathbf{F}_p(t)$ is algebraic. Since the automorphism σ maps $\mathbf{F}_p(t)$ onto $\mathbf{F}_p(\sigma(t))$, we have $[K : \mathbf{F}_p(t)] = [K : \mathbf{F}_p(\sigma(t))]$, and hence

$$d_\sigma = [\mathbf{F}_p(t, \sigma(t)) : \mathbf{F}_p(t)] = \frac{[K : \mathbf{F}_p(t)]}{[K : \mathbf{F}_p(t, \sigma(t))]} = \frac{[K : \mathbf{F}_p(\sigma(t))]}{[K : \mathbf{F}_p(t, \sigma(t))]}$$

$$= [\mathbf{F}_p(t, \sigma(t)) : \mathbf{F}_p(\sigma(t))] = h_\sigma. \quad \square$$

In Table 7 we give the state complexity for the automata we constructed (where the first two rows refer to series that are considered in the next section), plus the theoretical upper and lower bounds (computed using SINGULAR [31] and MAGMA [11]). We observe that the required number of states is much lower than the (generically almost tight, at least in the genus zero case) upper bounds. The reader may be convinced of this non-generic behaviour by perturbing some of the coefficients in the equation for σ_8 and using [14] to compute the number of states required to solve those perturbed equations (which typically also have higher genus).

Remark 9.2.2. Table 7 lacks a general formula for the minimal number of states in a 2-automaton computing Klopsch's series $\sigma_{\mathrm{K},m}$ for general m. For $m = 1, 3, 5, \ldots, 1023$ we computed this in [58] and [14] to be $2, 6, 14, 9, 28, 53, 67, 12, 54, 127, \ldots, 30$. One may show that for $m = 2^\mu - 1$ such an automaton has 3μ states. We conjecture that for $m = 2^\mu + 1$ it has $3 \cdot 2^\mu + 2\mu - 2$ states. For $m = 2^\mu + 3$, we find the sequence $14, 9, 53, 127, 90, 931, 2675, 770, \ldots$, which we could not fit into any mould.

10. A hierarchy of complexity of power series based on sparseness

Previously known examples of finite order elements of $\mathscr{N}(\mathbf{F}_2)$ were described as power series having as coefficients binomial coefficients modulo 2 (such as Klopsch's series) or by explicit formulas for the location of the nonzero coefficients (such as the Chinburg–Symonds series σ_{CS} and $\sigma_{\mathrm{CS}}^{\circ 3}$). Our automatic description is somewhat different. In this section, we discuss the relation between the existence of 'closed/explicit formulas' and properties of the automaton.

10.1. Sparse power series

We propose a definition of a 'closed formula' for a power series based on the notion of sparseness (the concept occurs in the literature under various names such as 'arid', 'poly-slender', 'polynomial growth', and 'bounded'; compare [18, §3]).

Definition 10.1.1. For a power series $\sigma = \sum a_k t^k \in \mathbf{F}_2[\![t]\!]$ over $\mathbf{F}_2$, let $E(\sigma)$ denote the *support* of σ, i.e. the set of integers k for which $a_k = 1$. A power series σ (as well as the corresponding automaton and automatic sequence, if they exist) is called *sparse* if

$$\#E(\sigma) \cap \{0, 1, \ldots, N\} = O(\log(N)^r)$$

for some $r \geqslant 0$. The infimum of such r is called the *rank of sparseness* of σ. We say that σ is r-sparse if the rank of sparseness is at most r. If σ is automatic, then this infimum is attained and is an integer (this follows from Proposition 10.1.3 below).

Note that polynomials are sparse, sums of sparse series are sparse, and products of sparse series are sparse. More precisely, if σ is r-sparse and τ is s-sparse, then $\sigma+\tau$ is at most $\max(r,s)$-sparse and $\sigma\tau$ is at most $(r+s)$-sparse; this follows from the definition, since $E(\sigma+\tau) \subseteq E(\sigma) \cup E(\tau)$ and $E(\sigma\tau) \subseteq E(\sigma) + E(\tau)$. For automatic sequences, Cobham showed the following dichotomy for the word growth in the associated regular language.

Proposition 10.1.2 *(Cobham [26]). An automatic sequence $\sigma \in \mathbf{F}_2[\![t]\!]$ is either sparse, or $\#E(\sigma) \cap \{0,1,\dots,N\} \geqslant N^{\alpha}$ for some real $\alpha > 0$ and sufficiently large N.* □

Define a *simple sparse set of rank at most r* to be a set of integers whose base-2 expansion is of the form $v_r w_r^{\ell_r} \cdots v_1 w_1^{\ell_1} v_0$ with $\ell_i \in \mathbf{Z}_{\geqslant 0}$ for some fixed binary words $v_0,\dots,v_r,w_1,\dots,w_r$.

Proposition 10.1.3 *(Szilard, Yu, Zhang and Shallit [63]). A series σ is automatic and sparse of rank at most r precisely if $E(\sigma)$ is a finite union of pairwise disjoint simple sparse sets of rank at most r.*

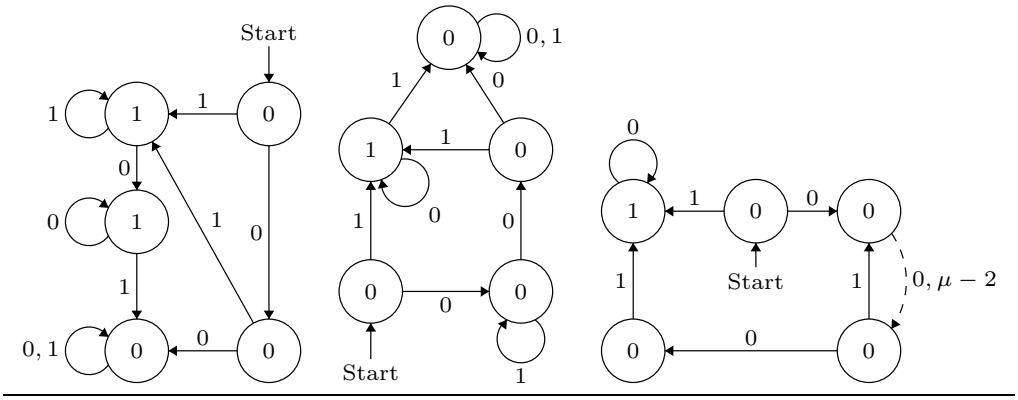
Proof. Except for the claim of 'pairwise disjointness', this is proven in [63]. The claim that the occurring simple sparse sets can be chosen pairwise disjoint is proven in detail in [18, Cor. 3.10]. □

Remark 10.1.4. The proof in [18, Cor. 3.10] is a tedious combinatorial verification. Jason Bell pointed out to us that a much simpler argument is possible if one uses the structure of the corresponding automaton that results from Proposition 12.1.2 below.

Example 10.1.5. The support of $\sigma_{\mathrm{CS}}^{\circ 3}$ is $E(\sigma_{\mathrm{CS}}^{\circ 3}) = \{3\cdot 2^k - 2 \mid k \geqslant 0\} \cup \{4\cdot 2^k - 2 \mid k \geqslant 0\}$, and consists of the integers whose base-2 expansion is 1, $101^{\ell}0$ or $1^{\ell}10$ for some $\ell \in \mathbf{Z}_{\geqslant 0}$. Similarly, all power series in Table 3 are sparse. On the other hand, the description of the support of $\sigma_{\mathrm{K},3}$ in Example 1.3.1 in terms of the base-4 representation with only half the possible digits allowed shows that $\#E(\sigma_{\mathrm{K},3}) \cap \{1,\dots,N\}$ grows as $\sqrt{N}f(N)$ for a function f that is bounded away from both 0 and infinity, and so $\sigma_{\mathrm{K},3}$ is not sparse.

Remark 10.1.6. A sparse automatic series is 'easy' in the sense that the full set consisting of the first N terms of the series can be computed in 'polylogarithmic time', i.e. polynomial time in $\log(N)$, given the words v_i, w_i as in the definition of a simple sparse set, which allow one to output the nonzero exponents in the series. In contrast to this, computation of the n-th coefficient of a general automatic sequence can be done in time $O(\log(n))$ (by base-2 expansion and running through the automaton), so computing all first N coefficients would require $O(\log(N!)) = O(N\log N)$ time.

Table 8
Automata corresponding to the power series $\sigma_{\mathrm{S},1}$ (left), $\sigma_{\mathrm{S},2}$ (middle) and $\sigma_{\mathrm{S},2^\mu-1}(\mu \geqslant 3)$ (right) in Proposition 10.2.1. The dashed arrow replaces a path consisting of $\mu-3$ vertices and $\mu-2$ edges, all with label zero. The remaining missing edges (in the right automaton) all connect to a unique vertex with label 0, which has been omitted in order to simplify the graphical representation of the automaton.



10.2. Conjugating to a sparse representative

One may ask whether every series of finite order in $\mathscr{N}(\mathbf{F}_2)$ can be conjugated to a sparse series. We have no general answer to this question, not even for series of order 2, which form a unique conjugacy class for every value of the break sequence (m), represented by Klopsch's series $\sigma_{\mathrm{K},m} = t/\sqrt[m]{1+t^m}$. Klopsch's series itself is not sparse, since its m-th power $\sigma_{\mathrm{K},m}^m = t^m/(1+t^m) = \sum_{k\geqslant 1} t^{km}$ is not. Nevertheless, for special values of the break sequence we can find a sparse representative.

Proposition 10.2.1. *Let m be an integer of the form $m = 2^\mu \pm 1$ for $\mu \geqslant 1$. Then any power series of order 2 and break sequence (m) is conjugate to a sparse power series. More precisely, we have the following*:

(i) Any power series of order 2 and break sequence (1) is conjugate to the power series

$$\sigma_{\mathrm{S},1} = t + \sum_{k\geqslant 2} \left(t^{2^k-2} + t^{2^k-1} \right), \tag{22}$$

which is sparse of rank 1. The corresponding automaton is displayed in Table 8.

(ii) If $m = 2^\mu - 1 > 1$, then any power series of order 2 and break sequence (m) is conjugate to the power series

$$\sigma_{\mathrm{S},m} = t + \sum_{k\geqslant 1} t^{\frac{m+1}{m-1}\left(m\cdot\left(\frac{m+1}{2}\right)^{k-1}-1\right)}, \tag{23}$$

which is sparse of rank 1. The set of exponents occurring in σ consists of the integers whose base-2 representation is either 1 or $10^{\mu-1}(10^{\mu-2})^\ell 0$ for some $\ell \in \mathbf{Z}_{\geqslant 0}$. The corresponding automata are displayed in Table 8.

(iii) *If $m = 2^\mu + 1$, then any power series of order 2 and break sequence (m) is conjugate to the power series*

$$\sigma_{\mathrm{S},m} = \sum_{\substack{\emptyset \neq J \subseteq \{0,\dots,\mu-1\} \\ k\colon J \to \mathbf{Z}_{\geqslant 0}}} t^{\left(\sum_{j\in J} 2^j (m-1)^{k(j)}\right) m - m + 1}, \tag{24}$$

which is sparse of rank μ: the support of $\sigma_{\mathrm{S},m}$ consists precisely of the integers $m(\ell-1)+1$ with $\ell \geqslant 1$ an integer whose base-2 expansion contains at most μ occurrences of the digit 1 and all these occurrences are at distinct positions modulo μ.

The crucial observation used in the proof is stated in the following lemma.

Lemma 10.2.2. *If a polynomial $F(t,X) = 0 \in \mathbf{F}_2[t,X]$ is symmetric in t and X, i.e. $F(t,X) = F(X,t)$, and, when regarded as an algebraic equation in X over $\mathbf{F}_2(\!(t)\!)$, has, for some $m \geqslant 1$, a unique solution $\sigma \in \mathscr{N}(\mathbf{F}_2)$ of the form $\sigma = t + t^{m+1} + O(t^{m+2})$, then σ is of order 2.*

Proof. Composing the equality $F(t,\sigma) = 0$ on the right with $\sigma^{\circ -1}$ gives $F(\sigma^{\circ -1}, t) = 0$, and hence, by symmetry of F, $F(t, \sigma^{\circ -1}) = 0$. Now note that if $\sigma = t + t^{m+1} + O(t^{m+2})$, then also $\sigma^{\circ -1} = t + t^{m+1} + O(t^{m+2})$. By uniqueness, it follows that $\sigma^{\circ -1} = \sigma$, so σ is of order 2. □

Proof of Proposition 10.2.1. We know that there is a unique conjugacy class of order-2 power series with a given break sequence (m), so it suffices to construct such a sparse series. When $m = 2^\mu \pm 1$, we will construct a sparse representative by exhibiting a symmetric algebraic equation $F(t,X) = 0$ over $\mathbf{F}_2$ as in Lemma 10.2.2. Choose the polynomial as follows:

$$\begin{cases} F(t,X) = (tX)^2 + (tX) + X + t & \text{for } m = 1; \\ F(t,X) = (tX)^{2^{\mu-1}} + X + t & \text{for } m = 2^\mu - 1 > 1; \\ F(t,X) = (tX)^{2^\mu} + X^{2^\mu - 1} + t^{2^\mu - 1} & \text{for } m = 2^\mu + 1. \end{cases}$$

In all cases, Hensel's Lemma implies the existence and uniqueness of a solution $\sigma = t + t^{m+1} + O(t^{m+2})$, so Lemma 10.2.2 applies. We can find an explicit solution iteratively, as follows.

For $m = 1$ we have

$$\sigma = \frac{t}{t+1} + \frac{t^2}{t+1}\sigma^2 = \frac{t}{t+1} + \frac{t^4}{(t+1)^3} + \frac{t^6}{(t+1)^3}\sigma^4 = \dots = \frac{t+1}{t^2}\sum_{k\geqslant 1} \frac{t^{3\cdot 2^{k-1}}}{(t+1)^{2^k}}.$$

The latter sum is

$$\sum_{k\geqslant 1}\frac{t^{3\cdot 2^{k-1}}}{(t+1)^{2^k}}=\sum_{k\geqslant 1}\sum_{m\geqslant 1}t^{(2m+1)\cdot 2^{k-1}}=\frac{t}{t+1}+\sum_{k\geqslant 1}t^{2^{k-1}},$$

leading to the stated formula for $\sigma=\sigma_{\mathrm{S},1}$.

For $m=2^\mu-1>1$, the same procedure leads to

$$\sigma_{\mathrm{S},m}=t+t^{2^{\mu-1}}\sigma^{2^{\mu-1}}=\cdots=t+\sum_{k\geqslant 0}t^{2^{\mu-1}+2^{2(\mu-1)}+\cdots+2^{k(\mu-1)}+2\cdot 2^{(k+1)(\mu-1)}},$$

which is equivalent to the stated formula.

Finally, for $m=2^\mu+1$, we let $\tau=t/\sigma$ and $q=2^\mu=m-1$. Then $\tau=1+O(t)$ satisfies

$$\tau=t^{q+1}+\tau^q \tag{25}$$

and hence

$$\tau=1+\sum_{k\geqslant 0}t^{q^k(q+1)}.$$

We find

$$t^q\sigma=1+\tau^{q-1}=1+\tau\cdot\tau^2\cdot\tau^4\cdots\tau^{2^{\mu-1}}=1+\prod_{j=0}^{\mu-1}\left(1+\sum_{k_j\geqslant 0}t^{(q+1)2^jq^{k_j}}\right),$$

which is equivalent to the stated formula. □

Remark 10.2.3. For odd $m\geqslant 1$ consider the degree-2 extension $\mathbf{F}_2(\!(z)\!)(x)$ of $\mathbf{F}_2(\!(z)\!)$ with $x^2+x=z^{-m}$. The element $t=xz^{\frac{m+1}{2}}$ is a uniformiser, and the generator σ of the Galois group acts by $\sigma(t)=(x+1)z^{\frac{m+1}{2}}$. We can eliminate the variables x and z by hand, obtaining the equation $(tX)^{\frac{m+1}{2}}+X+t=0$. This equation always has a unique solution in $\mathscr{N}(\mathbf{F}_2)$, which has depth m, but is not sparse unless $m+1$ is a power of 2 and $m\neq 1$ (this follows from Proposition 11.1.2 below).

Remark 10.2.4. The power series $\sigma_{\mathrm{S},1}$ from Proposition 10.2.1(i) is conjugate to Klopsch's series $\sigma_{\mathrm{K},1}:=t/(t+1)$. In this case, the conjugacy can be done using the simple *algebraic* power series $\chi=t/(t^2+1)$. Indeed, with $\psi:=\sum_{k\geqslant 1}t^{2^k-1}$, we have

$$\chi\cdot(\psi\circ\chi)=(t\cdot\psi)\circ\chi=\chi^2+\chi^4+\chi^8+\cdots=t^2/(t^2+1),$$

since the support of $t^2/(t^2+1)$ consists of all even integers, and the support of χ^{2^k} consists of the odd multiples of 2^k. Hence $\chi\cdot(\psi\circ\chi)=\chi\cdot t$, so $\chi^{\circ -1}=\psi$. We have $\chi\circ\sigma_{\mathrm{K},1}=t+t^2$, and hence

$$\chi \circ \sigma_{\mathrm{K},1} \circ \chi^{\circ -1} = \chi^{\circ -1} + (\chi^{\circ -1})^2 = \sum_{k \geqslant 1} t^{2^k - 1} + \sum_{k \geqslant 1} t^{2^{k+1}-2} = \sigma_{\mathrm{S},1}.$$

Remark 10.2.5. In Table 7, we have used that the genus of the smooth projective curve corresponding to $F(t, X) = (tX)^k + X + t$ is $k - 1$. This follows easily by the change of variables $t = y/x^k, X = x^{k-1}/y$, leading to the Artin–Schreier equation $y^2 + y = x^{2k-1}$, which has genus $k - 1$ (see e.g. [62, Thm. 6.4.1]). For the case $m = 2^\mu + 1$, we also used that the genus of the Artin–Schreier curve (25) is $2^{\mu-1}(2^\mu - 1)$.

Remark 10.2.6. We did not produce the general form of the automaton for $m = 2^\mu + 1$. Whereas the series for $m = 2^\mu - 1 > 1$ requires $\mu + 3 \approx \log(m)$ states and the rank of sparseness is 1, if $m = 2^\mu + 1$ an educated guess for the number of states of the minimal automaton is $2^\mu + 3^\mu \approx m^{\log(3)/\log(2)}$ and the rank of sparseness is (provably) μ. This looks somewhat similar to what happens with the Klopsch's series $\sigma_{\mathrm{K},m}$ for such values of m, cf. Remark 9.2.2. In all these families, the number of states appears to be logarithmic or polynomial in the genus, and never exponential, as is theoretically possibly by Bridy's bound discussed in Section 9.

10.3. Quasi-sparse series

Sparse series form an $\mathbf{F}_2[t]$-algebra that we will denote by S. Consider the larger $\mathbf{F}_2[t]$-algebra $\widehat{S}$ consisting of power series in $\mathbf{F}_2[\![t]\!]$ that can be written as products of sparse series and rational functions in $\mathbf{F}_2(t)$. Elements of this algebra can also be regarded as having nice 'closed formulas'. We have the following characterisation:

Proposition 10.3.1. *Let $\sigma = \sum_{k \geqslant 0} a_k t^k \in \mathbf{F}_2[\![t]\!]$ be a power series. The following conditions are equivalent*:

(i) $\sigma \in \widehat{S}$;
(ii) *there exists an integer $m \geqslant 1$ such that $(t^m + 1)\sigma$ is sparse*;
(iii) *there exists an integer $m \geqslant 1$ such that $\sum_{k \geqslant 0}(a_k + a_{k+m})t^k$ is sparse*;
(iv) *there exists an integer $m \geqslant 1$ such that $\sum_{k \geqslant 0}(a_k + a_{k+2^q m})t^k$ is sparse for all integers $q \geqslant 0$.*

Proof. Since sparse power series form a ring and include polynomials, $\sigma \in \widehat{S}$ if and only if there exists a nonzero $p \in \mathbf{F}_2[t]$ such that $p\sigma \in S$. Moreover, we may assume that p is not divisible by t since the class of sparse sequences in closed under shifts. The equivalence of (i) and (ii) then follows from the fact that every $p \in \mathbf{F}_2[t]$ that is not divisible by t divides the polynomial $t^m + 1$ for some $m \geqslant 1$: take $m = 2^k(2^r - 1)$ with r and k chosen so that the splitting field of p is $\mathbf{F}_{2^r}$ and every root of p has multiplicity $\leqslant 2^k$. The equivalence of (ii) and (iii), with the same value of m, is easy. Finally, the equivalence of (ii) and (iv) follows from the fact that if $(t^m + 1)\sigma$ is sparse, then so is $(t^m + 1)^{2^q}\sigma = (t^{2^q m} + 1)\sigma$ for all $q \geqslant 0$. □

A final operation that we allow without affecting our sense of 'admitting a closed formula' is for elements of $\widehat{S}$ to be twisted by an automorphism of $\mathbf{F}_2(t)$, as follows. There is a unique nontrivial field automorphisms of $\mathbf{F}_2(t)$ that is also an element of $\mathscr{N}(\mathbf{F}_2)$, given by the map

$$\varphi\colon t \mapsto t/(t+1).$$

The order of φ is two. It might happen that a power series $\sigma \in \mathscr{N}(\mathbf{F}_2)$ is not in S or $\widehat{S}$, but that $\sigma \circ \varphi$ is. This is equivalent with σ being in the algebra of sparse series *in the variable* $t/(t+1)$. Note that while composing with φ preserves the property of being an algebraic power series (if σ is a root of $F(t, X)$, then $\sigma \circ \varphi$ is a root of $F(\varphi(t), X)$), the property of being of finite order need not be preserved.

Definition 10.3.2. A series $\sigma = \sigma(t) \in \mathbf{F}_2[\![t]\!]$ is called *quasi-sparse* if either $\sigma \in \widehat{S}$ or $\sigma \circ \varphi \in \widehat{S}$. We denote the collection of quasi-sparse series by $\widehat{\widehat{S}}$.

This leads to a *hierarchy of complexity* for power series

$$S \subset \widehat{S} \subset \widehat{\widehat{S}} \subset \mathbf{F}_2[\![t]\!],$$

where every inclusion is strict. In the next two sections, we will study whether our series σ of finite order are in $S, \widehat{S}$ or $\widehat{\widehat{S}}$. The next section will employ field-theoretic methods, whereas the following one will be based purely on characterisations in terms of automata. We believe both methods have their merits.

11. Detecting sparseness properties using field theory

11.1. Field-theoretic characterisation of sparseness

Recently, Albayrak and Bell [4, Thm. 1.1(b)] gave an exact field-theoretic characterisation of sparseness for generalized (Hahn) power series in arbitrary positive characteristic. We will use a special case of one direction of their characterisation, of which we include a short, self-contained proof.

The following result will be used without further reference.

Lemma 11.1.1. *For any algebraic power series* $\tau \in \overline{\mathbf{F}}_2[\![t]\!]$*, the field extension* $\mathbf{F}_2(t)(\tau)/\mathbf{F}_2(t)$ *is separable.*

Proof. If the extension is not separable, the minimal polynomial $f \in \mathbf{F}_2(t)[X]$ of τ is of the form $f = \sum c_i(t) X^{2i}$. Since the Cartier operator satisfies $\mathscr{C}_r(\psi\tau^2) = \tau\mathscr{C}_r(\psi)$, applying this to the equation $f(\tau) = 0$, we find that $\sum \mathscr{C}_r(c_i(t))\tau^i = 0$. This gives a polynomial of strictly smaller degree satisfied by τ and nonzero for at least one value of $r \in \{0, 1\}$. This contradiction shows the result. □

Proposition 11.1.2 *(Albayrak–Bell [4], special case). Let $\sigma \in \mathscr{N}(\mathbf{F}_2)$ denote a power series that is algebraic over $\mathbf{F}_2(t)$. Consider the field*

$$\mathscr{F} = \bigcup_{\substack{\ell \geqslant 1, \\ \ell \text{ odd}}} \overline{\mathbf{F}}_2(t^{1/\ell}),$$

where $\overline{\mathbf{F}}_2$ is an algebraic closure of $\mathbf{F}_2$. If σ is sparse, then the following conditions hold:

(i) σ is integral over $\overline{\mathbf{F}}_2[t, t^{-1}]$;
(ii) the extension $\overline{\mathbf{F}}_2(t)(\sigma)/\overline{\mathbf{F}}_2(t)$ is unramified outside of $0, \infty$;
(iii) the splitting field of σ over $\mathscr{F}$ has degree a power of two.

Proof. The essence of the proof is to show that for sparse power series the combinatorial structure of the support $E(\sigma)$ allows one to construct a tower of Artin–Schreier extensions of $\mathscr{F}$ that contains σ.

By Proposition 10.1.3 a series σ is sparse precisely if $E(\sigma)$ is a finite union of pairwise disjoint simple sparse sets. Properties (i)–(iii) hold for the sum of several power series whenever they hold for the individual summands (for unramifiedness, use [62, Cor. 3.9.3]), and hence it is sufficient to prove that they hold for power series with simple sparse support. This will be done by induction on the rank of sparseness r.

Suppose that the support of σ is a simple sparse set, consisting of integers whose base-2 expansion is of the form $v_r w_r^{\ell_r} \cdots v_1 w_1^{\ell_1} v_0$ with $\ell_i \in \mathbf{Z}_{\geqslant 0}$ for some fixed binary words $v_0, \ldots, v_r$, and $w_1, \ldots, w_r$. If $r = 0$, then σ is a monomial, and properties (i)–(iii) hold. Suppose that $r \geqslant 1$ so w_1 is nontrivial. Let $k_0 = |v_0|$ and $k_1 = |w_1|$ be the lengths of the words v_0 and w_1, and let m_0 and m_1 be the integers whose base-2 expansion is v_0 and w_1. Let τ be the power series whose support consists of the integers with base-2 expansion of the form $v_r w_r^{\ell_r} \cdots w_2^{\ell_2} v_1 0^{k_0}$ with $\ell_i \in \mathbf{Z}_{\geqslant 0}$. By induction, we know that properties (i)–(iii) hold for τ. The relation between the supports of σ and τ leads directly to the formula

$$\sigma^{2^{k_1}} - t^{(2^{k_1}-1)m_0 - 2^{k_0} m_1} \sigma = t^{2^{k_1} m_0 - 2^{k_0} m_1} \tau. \tag{26}$$

This allows us to deduce the properties (i)–(iii) for σ from the corresponding properties of τ.

First of all, σ is integral over $\overline{\mathbf{F}}_2[t, t^{-1}][\tau]$, and hence also over $\overline{\mathbf{F}}_2[t, t^{-1}]$.

Secondly, the form of Equation (26) makes it very easy to compute the ramification of the extension $\overline{\mathbf{F}}_2(t)(\sigma)/\overline{\mathbf{F}}_2(t)(\tau)$. If f is the minimal polynomial of σ, then [62, Cor. 3.5.11] implies that the extension is unramified at all places P for which f is P-integral and $v_P(f'(\sigma)) = 0$. The same result then holds for any monic (not necessarily minimal) polynomial g satisfied by σ, since it is divisible by f. We apply this with g the polynomial in σ given in (26), and we find that the extension is unramified at all places P of $\overline{\mathbf{F}}_2(t)(\tau)$

with $v_P(t) = 0$ and $v_P(\tau) \geqslant 0$, and that for all places P' of $\overline{\mathbf{F}}_2(t)(\sigma)$ lying above such P we have $v_{P'}(\sigma) \geqslant 0$. This implies that $\overline{\mathbf{F}}_2(t)(\sigma)/\overline{\mathbf{F}}_2(t)$ is unramified outside of $0, \infty$.

Finally, multiplying Equation (26) by an appropriate (fractional) power of t leads to an equation of the form $(t^c\sigma)^{2^{k_1}} - (t^c\sigma) = t^d\tau$ for some c and d, which are rational numbers with odd denominators (more precisely, $c = -m_0 + \frac{2^{k_0}m_1}{2^{k_1}-1}$ and $d = \frac{2^{k_0}m_1}{2^{k_1}-1}$). This shows that the extension $\mathscr{F}(\sigma)/\mathscr{F}(\tau)$ is contained in a tower of Artin–Schreier extensions, and hence so is $\mathscr{F}(\sigma)/\mathscr{F}$. Thus, its Galois closure is of degree a power of two. □

11.2. Field-theoretic test for membership in the hierarchy

From Proposition 11.1.2, we can deduce a method for establishing that a series is not in S or $\widehat{S}$. Since the properties (ii) and (iii) depend only on the field $\overline{\mathbf{F}}_2(t)(\sigma)$, and not on σ itself, any proof that uses them to show that $\sigma \notin S$ will establish the stronger property that $\sigma \notin \widehat{S}$. Actually, the method we will use to show that for a particular σ property (iii) does not hold will even show that $\sigma \notin \widehat{\widehat{S}}$. On the other hand, the integrality property (i) will be used to show that certain series are in $\widehat{S}$, but not in S.

The basic ingredient is the following field-theoretic result, restricting possible factorisations of polynomials after extension of the base field.

Lemma 11.2.1. *Let L/K be a (possibly infinite) Galois extension with Galois group G, let $f \in K[X]$ be a monic irreducible polynomial, and let $g \in L[X]$ be a monic irreducible factor of f in $L[X]$. Denote by H the stabiliser of g in G. Then*

$$f = \prod_{\phi \in G/H} g^{\phi},$$

i.e. f is the product of all (pairwise distinct) Galois conjugates g^{ϕ} for ϕ running through the coset space G/H.

Proof. Let α denote a root of g in an algebraic closure of L; then g is the minimal polynomial of α over L. Put $\tilde{f} := \prod g^{\phi}$, the product being taken over all ϕ running through the coset space G/H. By construction, $\tilde{f}$ lies in $K[X]$ and has α as a root, hence f divides $\tilde{f}$. Conversely, g divides f in $L[X]$, and hence so does g^{ϕ} for all $\phi \in G$. Since the elements g^{ϕ} are irreducible and pairwise distinct for $\phi \in G/H$, the polynomial $\tilde{f}$ divides f. Hence, $f = \tilde{f}$. □

This implies the following valuation-theoretic result that can be used to check whether a polynomial stays irreducible under base field extension.

Lemma 11.2.2. *Let L/K be a (possibly infinite) Galois extension with Galois group G, and let $v\colon L \to \mathbf{R} \cup \{\infty\}$ be an (additive) valuation that is G-invariant, in the sense that $v \circ \phi = v$ for all $\phi \in G$. Let $\overline{L}$ be an algebraic closure of L, and let $\tilde{v}$ be an extension of the*

valuation v to $\overline{L}$. For a polynomial $f \in K[X]$, denote by $V_v(f)$ the multiset of valuations $\tilde{v}(\alpha)$ of all the roots α of f in $\overline{L}$. If f is irreducible over K, but becomes reducible over L, then the multiplicities of the elements of $V_v(f)$ have a nontrivial common divisor.

Elements of the set $V_v(f)$ are minus the slopes of the Newton polygon $\mathrm{NP}(f)$ of $f = \sum_{i=0}^{n} a_i X^i$, where $\mathrm{NP}(f)$ is given as the lower convex hull in $\mathbf{R}^2$ of the set of points $(i, v(a_i))$ for $0 \leqslant i \leqslant n$.

Proof. Since we assume that $v \circ \phi = v$, we have $\mathrm{NP}(g^\phi) = \mathrm{NP}(g)$. Since the multiset $V_v(h)$ of a polynomial h is determined by its Newton polygon (and hence by the valuations of its coefficients), it follows from the decomposition $f = \prod g^\phi$ as in Lemma 11.2.1 that $V_v(f)$ is the union of $[G : H] > 1$ copies of $V_v(g)$ (as multisets). □

Proposition 11.2.3. *Let $f \in \mathbf{F}_2(t)[X]$ be a separable irreducible polynomial. If the multiplicities of the elements of the multiset $V_t(f)$ for the t-adic valuation have no nontrivial common divisor, then f remains irreducible over $\mathscr{F}$.*

Proof. The extension $\mathscr{F}/\mathbf{F}_2(t)$ is Galois. The t-adic valuation on $\mathbf{F}_2(t)$ has a unique extension to $\mathscr{F}$ (which coincides on each $\overline{\mathbf{F}}_2(t^{1/j})$ with the $t^{1/j}$-adic valuation v normalised so that $v(t^{1/j}) = 1/j$). By uniqueness, this extension is Galois invariant. The claim follows from Lemma 11.2.2. □

Corollary 11.2.4. *Let $\sigma \in \mathscr{N}(\mathbf{F}_2)$ denote a power series that is algebraic over $\mathbf{F}_2(t)$ with minimal polynomial $F(t, X)$. Assume that F is of degree not a pure power of two, and that the multiplicities of the elements of the multiset $V_t(\sigma) := V_t(F)$ for the t-adic valuation have no nontrivial common divisor. Then $\sigma \notin \widehat{\widehat{S}}$.*

Proof. We conclude from Proposition 11.2.3 that F is the minimal polynomial of σ over $\mathscr{F}$, and so $[\mathscr{F}(\sigma) : \mathscr{F}]$ is not a pure power of two, contradicting Proposition 11.1.2(iii). Hence $\sigma \notin S$. Since the field $\mathscr{F}(\sigma)$ does not change after multiplying σ by a rational function, we get that $\sigma \notin \widehat{S}$.

For the final claim, observe that replacing σ by $\sigma \circ \varphi$ changes neither the degree of the minimal polynomial of σ over $\mathbf{F}_2(t) = \mathbf{F}_2(t/(t+1))$ nor the set $V_t(\sigma)$. Hence the same reasoning applied to $\sigma \circ \varphi$ shows that $\sigma \notin \widehat{\widehat{S}}$. □

Corollary 11.2.5. *Let $\sigma \in \mathscr{N}(\mathbf{F}_2)$ denote a power series that is algebraic over $\mathbf{F}_2(t)$ with minimal polynomial $F(t, X)$ of degree 4*

$$F(t, X) = a_4 X^4 + a_3 X^3 + a_2 X^2 + a_1 X + a_0$$

and with cubic resolvent

$$R_3[F] := a_4^3 X^3 + a_2 a_4^2 X^2 + a_1 a_3 a_4 X + a_0 a_3^2 + a_1^2 a_4.$$

Assume that $R_3[F]$ is irreducible over $\mathbf{F}_2(t)$ and that the multiplicities of the elements of the multisets $V_t(F)$ and $V_t(R_3[F])$ for the t-adic valuation have no nontrivial common divisor. Then $\sigma \notin \widehat{\widehat{S}}$.

Proof. The possible Galois groups of an irreducible separable quartic are S_4, A_4 D_4, $\mathbf{Z}/4\mathbf{Z}$ and $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Only the last three of these are 2-groups, and those occur precisely when the cubic resolvent is reducible (see [27, Thm. 3.4]).

Since F is separable, so is its cubic resolvent $R_3[F]$. From the hypotheses and Proposition 11.2.3, we conclude that F and $R_3[F]$ are irreducible over $\mathscr{F}$. Therefore, the Galois group of σ over $\mathscr{F}$ is not a 2-group, and $\sigma \notin S$ by Proposition 11.1.2(iii). Since this argument uses only the information about the field $\mathscr{F}(\sigma)$, we conclude that $\sigma \notin \widehat{S}$.

Finally, since changing σ to $\sigma \circ \varphi$ affects neither the irreducibility of F and $R_3[F]$ nor the sets $V_t(F)$ and $V_t(R_3[F])$, we find similarly that $\sigma \circ \varphi \notin \widehat{S}$, and so $\sigma \notin \widehat{\widehat{S}}$. □

Theorem 11.2.6. *We have the following membership properties (see also Table 9)*:

(i) $\sigma_{\mathrm{S},2^\mu \pm 1} (\mu \geqslant 1), \sigma_{\mathrm{CS}}^{\circ 3}, \sigma_{\mathrm{T},1}, \ldots, \sigma_{\mathrm{T},4} \in S$;
(ii) $\sigma_{\mathrm{CS}}^{\circ 2}, \sigma_{\mathrm{CS}} \in \widehat{S} \setminus S$;
(iii) $\sigma_{\mathrm{J}}, \sigma_{\mathrm{J}}^{\circ 3} \in \widehat{\widehat{S}} \setminus \widehat{S}$;
(iv) $\sigma_{\mathrm{K},m} (m \geqslant 3), \sigma_{V,1}, \sigma_{V,2}, \sigma_{V,3}, \sigma_{\min}, \sigma_{(1,5)}, \sigma_{(1,9)}, \sigma_8 \notin \widehat{\widehat{S}}$.

Proof. The series $\sigma_{\mathrm{S},2^\mu \pm 1}$ are sparse by Proposition 10.2.1. The sparseness of the series $\sigma_{\mathrm{CS}}^{\circ 3}$, $\sigma_{\mathrm{T},1}, \ldots, \sigma_{\mathrm{T},4}$ follows by representing $E(\sigma)$ in the same way as was done for $E(\sigma_{\mathrm{CS}}^{\circ 3})$ in Example 10.1.5, using the closed formulas for the series in Table 3.

The series $\sigma_{\mathrm{CS}}^{\circ 2}$ and σ_{CS} are not sparse by Proposition 11.1.2 since their minimal polynomials are not $\overline{\mathbf{F}}_2[t, t^{-1}]$-integral. To show the series are in $\widehat{S}$, we have the following explicit relations, obtained from Remark 5.1.4 and Equation (12), with sparse right hand side:

$$(t+1)^2 \sigma_{\mathrm{CS}}^{\circ 2} = t + t^3 + \sum_{k \geqslant 1} \left(t^{2 \cdot 2^k} + t^{3 \cdot 2^k} \right) \qquad \text{and} \qquad (t+1)^2 \sigma_{\mathrm{CS}} = \sum_{k \geqslant 0} \left(t^{2^k} + t^{3 \cdot 2^k} \right).$$

If σ is any of the series σ_{J} and $\sigma_{\mathrm{J}}^{\circ 3}$, then it is not in $\widehat{S}$. Indeed, from their minimal polynomial we can read out that the extension $\overline{\mathbf{F}}_2(t)(\sigma)/\overline{\mathbf{F}}_2(t)$ is ramified above $t+1$, and the conclusion follows from Proposition 11.1.2(ii). To prove the series are in $\widehat{\widehat{S}}$, we use the following explicit relations with sparse right hand side:

$$(t+1)\sigma_{\mathrm{J}}(\varphi(t)) = (t+1)^2 \sigma_{\mathrm{CS}}(t) \qquad \text{and} \qquad (t^2+t)\sigma_{\mathrm{J}}^{\circ 3}(\varphi(t)) = \sum_{k \geqslant 0} \left(t^{3 \cdot 2^k} + t^{2 \cdot 2^k} \right).$$

Indeed, for the former equation, one verifies that σ_{CS} and $\sigma_{\mathrm{J}}(\varphi(t))/(t+1)$ are equal, since they satisfy the same irreducible algebraic equation (12) having a unique solution

$t+O(t^2)$. For the latter equation, the left hand side is the unique solution to $\tau^2+\tau = t^3+t^2$ of the form $t^2 + O(t^3)$. But this solution is clearly equal to the right hand side.

To prove that $\sigma_{\mathrm{K},m} \notin \widehat{S}$ for any odd $m \geqslant 3$, we use Proposition 11.1.2(iii). To this end, it suffices to check that $(t^m + 1)X^m + t^m$ is irreducible over $\mathscr{F}$, which by [62, Prop. 3.7.3] is equivalent to showing that $t^m/(t^m + 1)$ is not a d-th power in $\mathscr{F}$ for any $d > 1$, $d|m$, or, equivalently, that $t^{mj}/(t^{mj} + 1)$ is not a d-th power in $\mathbf{F}_2(t)$ for any odd j. This holds since $t^{mj} + 1$ has only simple roots in $\overline{\mathbf{F}}_2$. Similarly, $\sigma_{\mathrm{K},m} \circ \varphi$ satisfies $(t^m+(t+1)^m)X^m+t^m = 0$, and the polynomial $t^{mj}+(t+1)^{mj}$ has only simple roots in $\overline{\mathbf{F}}_2$ (as can be seen from computing its derivative); hence for the same reason $\sigma_{\mathrm{K},m} \circ \varphi \notin \widehat{S}$. We conclude that $\sigma_{\mathrm{K},m} \notin \widehat{\widehat{S}}$.

The multisets of slopes for the minimal polynomials of $\sigma_{V,1}$, $\sigma_{V,2}$ and $\sigma_{V,3}$ can be found in Table 9. The cubic resolvent for the minimal polynomial of $\sigma_{V,1}$ is $t^{12}X^3 + t^8X^2 + t^7(t + 1)X + t^4(t^4 + t^3 + t^2 + 1)$, which is irreducible over $\mathbf{F}_2(t)$ with v_t-slopes $\{-4, (-2)^2\}$. (A convenient way to check irreducibility of the cubic resolvent over $\mathbf{F}_2(t)$ is to consider the $v_{t^{-1}}$-slopes for the t^{-1}-adic valuation.) Similarly, the minimal polynomial for $\sigma_{V,2}$ has resolvent $(t + 1)^{12}X^3 + t(t + 1)^8X^2 + (t + 1)^4t^4$, which is irreducible over $\mathbf{F}_2(t)$ and has v_t-slopes $\{1, (3/2)^2\}$, and the minimal polynomial for $\sigma_{V,3}$ has resolvent $t^{12}X^3+t^9(t^2+t+1)X^2+t^4(t+1)^6X+t(t+1)^6(t^3+t^2+1)$, which is irreducible over $\mathbf{F}_2(t)$ and has v_t-slopes $\{(-4)^2, -3\}$. By Corollary 11.2.5 we conclude that $\sigma_{V,1}, \sigma_{V,2}, \sigma_{V,3} \notin \widehat{\widehat{S}}$.

For all further series, $\deg F$ is not a pure power of 2 and $V_t(F)$ has no nontrivial common divisor of multiplicities (listed in Table 9), so we immediately conclude that $\sigma \notin \widehat{\widehat{S}}$ by Corollary 11.2.4. This finishes the proof. □

12. Sparseness and automaton properties

12.1. Combinatorial characterisation of sparseness

We describe automaton-theoretic methods to verify whether a series σ is in $S, \widehat{S}$ or $\widehat{\widehat{S}}$. In [63], it is shown that sparseness may be checked directly using a corresponding automaton (recall our convention that all states in the automaton are accessible, which is also part of the conditions below).

Definition 12.1.1. Call a vertex v of an automaton *tied* if the following two properties hold:

(a) there exists a (possibly empty) path from v to a vertex with output 1 [‘v is co-accessible’];
(b) there exist two different walks of the same length from v to itself.

Proposition 12.1.2 *([63], [18, Prop. 3.4]). An automatic series σ is not sparse if and only if there exists a tied vertex v in a corresponding automaton.* □

This criterion can be used immediately to verify that the series $\sigma_{\mathrm{S},2^\mu-1}(\mu \geqslant 1)$, $\sigma_{\mathrm{CS}}^{\circ 3}$, $\sigma_{\mathrm{T},1}, \ldots, \sigma_{\mathrm{T},4}$ are sparse.

Example 12.1.3. The 2-automaton A corresponding to the expansion of the series $(1+t)^{-1/m}$ can be succinctly described as follows. Let ϖ denote the multiplicative order of 2 modulo m and consider the base-2 expansion $(2^\varpi - 1)/m = \sum_{i=0}^{\varpi-1} x_i 2^i$. The set of vertices of A is $\{v_0, \ldots, v_{\varpi-1}, w\}$. All v_j have vertex label 1, w has vertex label 0, and v_0 is the start vertex. For any j, v_j is connected to $v_{j+1 \bmod \varpi}$, always by an edge with label 0, and by an edge with label 1 exactly if $x_j = 1$. If $x_j = 0$, an edge with label 1 connects v_j to w. Finally, w has two self-loops labelled 0 and 1. The automaton A is not sparse since any vertex v_j with $x_j = 1$ is not tied: 0^ϖ and $0^{\varpi-1}1$ are two paths that satisfy condition (b). (This incidentally provides another proof of the non-sparseness of Klopsch's series $\sigma_{\mathrm{K},m}(t) = t/\sqrt[m]{1+t^m}$; however, we do not have a synthetic description for an automaton corresponding to $\sigma_{K,m}$ for general m and, in particular, do not have a formula for the minimal number of states as a function of m, cf. Table 7.)

A similar description of a minimal p-automaton for $(1+at)^{-1/m} \in \mathbf{F}_p[\![t]\!]$ for any prime p, m coprime to p and $a \in \mathbf{F}_p^*$ is given in [64].

12.2. Combinatorial tests for membership in the hierarchy

We have not been able to find a necessary and sufficient condition for a series to be in $\widehat{S}$ in terms of the automaton alone. We will however give a simple necessary criterion, from which one may deduce all statements in Theorem 11.2.6, *except* the facts that $\sigma_{\min} \notin \widehat{S}$ and $\sigma_{(1,9)} \circ \varphi \notin \widehat{S}$.

In applying the criterion, it is necessary to move the 'start' label to other vertices. This might produce non-accessible vertices, which should then be removed from the automaton; this does not affect the resulting automatic sequence.

Proposition 12.2.1. *Let $\sigma(t) = \sum_{k\geqslant 0} a_k t^k \in \mathbf{F}_2[\![t]\!]$ be a power series generated by an automaton A. Then $\sigma(t) \notin \widehat{S}$ if there exists a vertex v in A satisfying the following two properties*:

(i) there exist arbitrarily long walks from the start vertex to v;
(ii) let v_0 and v_1 denote the vertices reached by following the edge starting at v and labelled 0 and 1, respectively, and let A_i be the automaton obtained from A by changing the start vertex to v_i. Then exactly one of the automata A_0 and A_1 is sparse (and the other one is not sparse).

Remark 12.2.2. Since the automaton is finite, the existence of arbitrarily long walks from the start vertex to v is equivalent to the existence of paths w_0, w_1 and w_2 such that w_1 is nontrivial and for every integer $\ell \geqslant 0$ the walk $w_2 w_1^\ell w_0$ goes from the start vertex to v.

Table 9
For each series, in column '$\in S$' the symbol '$\times$' indicates the series is not sparse and '$\checkmark(r)$' indicates the series is r-sparse; the column '$\in \widehat{S}$' describes the property of being sparse up to multiplication with a rational function; the column '$\in \widehat{\widehat{S}}$' indicates whether or not the series itself or its composition with $t \mapsto t/(t+1)$ is in $\widehat{S}$; 'minimal polynomial F' is the minimal polynomial of the series over $\mathbf{F}_2(t)$; 'method' indicates the method of proof, where $V_t := V_t(F)$ is the multiset of t-adic valuations of the roots of F.

series	$\in S$	$\in \widehat{S}$	$\in \widehat{\widehat{S}}$	minimal polynomial F	method
$\sigma_{\mathrm{S},1}$	$\checkmark(1)$	$\checkmark$	$\checkmark$	$t^2X^2 + (t+1)X + t$	direct
$\sigma_{\mathrm{S},m=2^\mu-1>1}$	$\checkmark(1)$	$\checkmark$	$\checkmark$	$(tX)^{(m+1)/2} + X + t$	direct
$\sigma_{\mathrm{S},m=2^\mu+1}$	$\checkmark(\mu)$	$\checkmark$	$\checkmark$	$(tX)^{m-1} + X^{m-2} + t^{m-2}$	direct
$\sigma_{\mathrm{CS}}^{\circ 3}$	$\checkmark(1)$	$\checkmark$	$\checkmark$	$t^2X^2 + X + t^2 + t$	direct
$\sigma_{\mathrm{T},1}$	$\checkmark(2)$	$\checkmark$	$\checkmark$	$t^2X^4 + (t^4+t^2+t+1)X^2 + (t^3+t^2+t)X + t^3$	direct
$\sigma_{\mathrm{T},2}$	$\checkmark(3)$	$\checkmark$	$\checkmark$	$t^2X^4 + (t+1)X^3 + (t^4+t^2+t)X^2 + (t^2+t)X + t^2$	direct
$\sigma_{\mathrm{T},3}, \sigma_{\mathrm{T},4}$	$\checkmark(3)$	$\checkmark$	$\checkmark$	$t^4X^4 + (t^2+1)X^3 + (t^3+t)X^2 + t^2X + t^3$	direct
$\sigma_{\mathrm{CS}}^{\circ 2}$	$\times$	$\checkmark$	$\checkmark$	$(t+1)^2X^2 + X + t^2 + t$	not integral
σ_{CS}	$\times$	$\checkmark$	$\checkmark$	$(t+1)^2X^2 + X + t$	not integral
σ_{J}	$\times$	$\times$	$\checkmark$	$(t+1)X^2 + (t^2+1)X + t$	not unramified
$\sigma_{\mathrm{J}}^{\circ 3}$	$\times$	$\times$	$\checkmark$	$tX^2 + (t^2+1)X + t^2 + t$	not unramified
$\sigma_{\mathrm{K},m}$	$\times$	$\times$	$\times$	$(t^m+1)X^m + t^m$	odd deg & direct
$\sigma_{V,1}$	$\times$	$\times$	$\times$	$t^4X^4 + t^3X^3 + X^2 + (t+1)X + t^2 + t$	R_3 & $V_t = \{(-2)^2, 0, 1\}$
$\sigma_{V,2}$	$\times$	$\times$	$\times$	$(t+1)^4X^4 + tX^2 + t^2X + t^4$	R_3 & $V_t = \{(\frac{1}{2})^2, 1, 2\}$
$\sigma_{V,3}$	$\times$	$\times$	$\times$	$t^4X^4 + (t+1)^3X^3 + t(t^2+t+1)X^2 + (t+1)^3X + t(t+1)^2$	R_3 & $V_t = \{-4, 0^2, 1\}$
$\sigma_{\min}$	$\times$	$\times$	$\times$	$(t+1)^3X^3 + (t^3+t)X^2 + (t^3+t+1)X + t^3 + t$	odd deg & $V_t = \{0^2, 1\}$
$\sigma_{(1,5)}$	$\times$	$\times$	$\times$	$t^2X^3 + (t+1)^3X + t^3 + t$	odd deg & $V_t = \{(-1)^2, 1\}$
$\sigma_{(1,9)}$	$\times$	$\times$	$\times$	$t^2X^7 + t^3X^6 + (t^5+t^4+t^2)X^5 + (t^5+t^3)X^4 +$ $+(t^7+t^5+t^4+t^3+t)X^3 + t^5X^2 + (t^3+t+1)X + t$	odd deg & $V_t = \{(-\frac{1}{3})^6, 1\}$
σ_8	$\times$	$\times$	$\times$	$t^6X^6 + (t^6+t^2)X^4 + (t^6+t^5+t^4+t^3+t^2+1)X^2 +$ $+(t+1)^3X + t^6 + t^5 + t^2 + t$	deg not a power of 2 & $V_t = \{(-2)^2, (-1)^2, 0, 1\}$

Proof of Proposition 12.2.1. For the purpose of the proof, we let $(n)_2$ denote the base-2 expansion of an integer $n \geqslant 0$.

Consider a walk from the start vertex to v, say of length ℓ, and let w be the binary word given by the concatenation of its labels. Let c be the integer such that $(c)_2 = w$. It follows directly from the definition that the automatic sequences produced by A_0 and A_1 are $(a_{2^{\ell+1}n+c})_{n\geqslant 0}$ and $(a_{2^{\ell+1}n+2^\ell+c})_{n\geqslant 0}$, respectively. Let $i \in \{0,1\}$ be such that the automaton A_i is not sparse; the automaton A_{1-i} is then sparse.

Let $m \geqslant 1$ be a fixed arbitrary odd integer. Consider integers k of the form $k = k(n) = 2^{\ell+1}n + 2^\ell i + c$ (where ℓ and $i = 0, 1$ are fixed while n runs through $\mathbf{Z}_{\geqslant 0}$). The base-2 expansion of $k + 2^\ell m$ is of the form $(k + 2^\ell m)_2 = u(1-i)w$ for some binary word u, and hence the walk given by it leads from the start vertex to a vertex in A_{1-i}. Since A_{1-i} is sparse, the number of $n \leqslant N$ such that $a_{k+2^\ell m} = 1$ grows as $O(\log(N)^r)$ for some $r \geqslant 0$. On the other hand, the base-2 expansion of k is $(k)_2 = (n)_2 iw$, the automaton A_i is not sparse, and hence the number of $n \leqslant N$ such that $a_k = 1$ grows faster than $\log(N)^r$ for any $r \geqslant 0$, and so does the number of n such that $a_k + a_{k+2^\ell m} = 1$. It follows that the power series

$$\sum_{n\geqslant 0} \left(a_{k(n)} + a_{k(n)+2^\ell m}\right) t^n$$

is not sparse, and hence neither is the series

$$\sum_{n\geqslant 0} \left(a_n + a_{n+2^\ell m}\right) t^n.$$

Since the integer $m \geqslant 1$ was arbitrary odd, and since the walk from the start vertex to v can be chosen with ℓ arbitrarily large, we conclude from Proposition 10.3.1(iv) that σ is not in $\widehat{S}$. □

A heuristics to apply Proposition 12.2.1 is now as follows. To verify that one of the automata A_0, A_1 is non-sparse, we can use Proposition 12.1.2; for this one can use cycle-finding algorithms. The tricky part is to verify that the other automaton is sparse—to this end, we need to exclude the existence of appropriate walks in the graph. To simplify this problem one may insist that the sparse of the automata A_0, A_1 be very simple; in fact, in all the examples discussed below it is possible to find such an automaton consisting of only one state, with label 0, making the verification obvious. Inverting this logic, we can hope to apply the criterion by first finding a vertex w with label 0 and two self-loops (a so-called 'absorbing state', cf. Section 13 below), and then going through all the vertices v admitting an edge from v to w, and checking if any of them satisfies the conditions of Proposition 12.2.1.

Sketch of a second proof of (part of) Theorem 11.2.6. The verification that certain series belong to $S, \widehat{S}$ or $\widehat{\widehat{S}}$ is direct and the same as in the first proof. The verification that

Table 10
'path' indicates a path from the start vertex to a tied vertex; 'path to vertex with output 1' indicates a path from the tied vertex to a vertex with output 1; p_1 and p_2 are walks of the same length that connect the tied vertex to itself, indicating that the series in non-sparse; ϵ indicates the empty path.

series	path	path to vertex with output 1	(p_1, p_2)
σ_{CS}	0	1	$(101, 100)$
$\sigma_{\mathrm{CS}}^{\circ 2}$	0	10	$(1101, 1110)$
$\sigma_{\min}$	1	ϵ	$(011, 100)$

certain series do not belong to $S, \widehat{S}$ or $\widehat{\widehat{S}}$ can be done by studying the corresponding automata and using Propositions 12.1.2 and 12.2.1. We have summarised some of the combinatorial data for this in Tables 10 & 11. For small automata, these data can be easily found just by looking at the graphical representation. This is the case for all the series in Tables 10 & 11 except for $\sigma_{(1,9)}$. To illustrate how one can use a computer algebra system to find these data for larger automata, we have written a MATHEMATICA notebook doing this for the series $\sigma_{(1,9)}$, generated by an automaton with 110 states, see [17].

To verify that a series is not in S, one indicates a path from the start vertex to a tied vertex v and two different walks of the same length from v to itself. One also checks that v is co-accessible by indicating a path from v to a vertex with output 1. These data are gathered in Table 10.

To verify that a series is not in $\widehat{S}$ one indicates paths w_0, w_1, w_2 such that every walk $w_2 w_1^{\ell} w_0$ leads from the start vertex to the same vertex v; a digit $i \in \{0, 1\}$ such that the automaton A_i (resp. A_{1-i}) obtained by moving the start vertex to the endpoint v_i of the edge starting at v and labelled i is non-sparse (resp. sparse); a path from v_i to a tied vertex; a path from that tied vertex to a vertex with output 1; and different walks of the same length from the tied vertex to itself, verifying that the automaton A_i is non-sparse. In all the cases listed in Table 11 the vertex v_{1-i} has label zero and two self-loops, implying that the automaton A_{1-i} is sparse, and providing the final step of the verification that the considered series is not in $\widehat{S}$.

We have listed the combinatorial data only for some of the series, but a similar procedure can be performed for all the series considered in Table 9 except $\sigma_{\min}$ and $\sigma_{(1,9)} \circ \varphi$, which are not in $\widehat{S}$, but for which the criterion from Proposition 12.2.1 is not satisfied. □

Remark 12.2.3. Since the class $\widehat{S}$ contains all power series whose coefficients are ultimately periodic, an automaton-theoretic criterion for membership in $\widehat{S}$ gives a necessary criterion for ultimate periodicity. It is known how to test for ultimate periodicity algorithmically, e.g. by work of Honkala [40] (this reference is phrased in a different, but equivalent language, where, for series over a binary alphabet, 'p-automatic' is 'p-recognisable' and 'ultimately periodic' is 'recognisable', or p-recognisable for all p, by

Table 11
The words w_i are the words needed to apply Remark 12.2.2; 'edge to non-sparse' has value $i \in \{0,1\}$ if the automaton A_i considered in Proposition 12.2.1 is non-sparse; 'path' indicates a path from the vertex v_i from Proposition 12.2.1 to a tied vertex; 'path to vertex with output 1' indicates a path from the tied vertex to a vertex with output 1; p_1 and p_2 are walks of the same length that connect the tied vertex to itself, indicating that the series is not in $\widehat{S}$; ϵ indicates the empty path.

series	(w_2, w_1, w_0)	edge to non-sparse	path	path to vertex with output 1	(p_1, p_2)
σ_{J}	$(1, 0, 00)$	1	ϵ	ϵ	$(0, 1)$
$\sigma_{\mathrm{J}}^{\circ 3}$	$(1, 0, 001)$	1	ϵ	ϵ	$(0, 1)$
$\sigma_{V,1}$	$(1, 0{,}000)$	0	ϵ	1	$(1001, 0100)$
$\sigma_{V,2}$	$(1, 0, 1)$	0	ϵ	1	$(1001, 0100)$
$\sigma_{\mathrm{K},3}$	$(\epsilon, 00, 0)$	0	01	ϵ	$(00, 11)$
$\sigma_{(1,5)}$	$(1, 0, 001)$	0	1	ϵ	$(11001, 01011)$
$\sigma_{(1,9)}$	$(0^5 1010, 1, 1^3 0^3)$	1	001	1	$(0^2 1^2 0^5 1^2 0^2 10^2 101^2 0^2,$ $0^3 1^2 0^2 10^2 101^2 0^4 1^2 0^2)$

Cobham's theorem [25].) The algorithm involves constructing another non-deterministic automaton and determinising it. It might be that one may find a similar algorithm for membership in $\widehat{S}$. Nevertheless, this seems to indicate that 'seeing' membership in $\widehat{S}$ directly from the automaton might be hard.

13. 'Non-randomness' of the series and synchronisability of the automata

13.1. Synchronising automata

Recall that an automaton is called *synchronising* if there is an input string (a 'synchronising word' p_{sync}), which, when followed from an arbitrary vertex, always leads to the same end vertex; this means that the word resets the automaton—if the base-2 expansion of n contains the word p_{sync}, the corresponding coefficient a_n depends only on the part of the expansion that is to the left of the occurrence of p_{sync}.

Example 13.1.1. The word 1011 is synchronising for $\sigma_{\mathrm{K},3}$. Following this word (right to left) starting at any state of the automaton leads to the state in the middle of the bottom row of Fig. 1.

Synchronisation is particularly easy to check when there is an *absorbing state* v, meaning that both outgoing edges from v are loops.

Lemma 13.1.2. *If an automaton A has an absorbing state v, then A is synchronising if and only if for any vertex w in A there is a path from w to v (in particular, A is not synchronising if there is more than one absorbing state).*

Proof. Since v is mapped to itself by any word, the synchronising word should map any vertex to v. In particular, for A to be synchronising, any vertex needs to be connected by a path to v. If this holds, choose an input string p for which the number of end vertices

of all paths with label p and arbitrary beginning vertex is minimal. If the only such end vertex is the absorbing state v, p is a synchronising word. If not, let v_1 denote another such end vertex and choose a path p_1 from v_1 to v (which exists by assumption). Now, the number of end vertices of paths with label p_1p is strictly smaller than for p (since both v_1 and v are connected to v by a path with label p_1), contradicting the minimality. □

As the number N tends to infinity, the fraction of synchronising automata with N states tends to 1 [7], but the fraction of automata with N states having an absorbing state tends to 0. The next lemma shows something very different happens for the class of minimal *sparse* automata.

Lemma 13.1.3. *If an automaton A is minimal and sparse, then A has a unique absorbing state v, and for any vertex w in A there is a path from w to v.*

Proof. Call any maximal subgraph of A that is connected as a directed graph a *strongly connected component*. For example, any absorbing state is a strongly connected component.

Let U denote the union of all strongly connected components. For any vertex v of A let $n(v)$ be the number of vertices that can be reached from v by following some directed path. It is easy to see that if for some vertex w there is a path from v to w, then $n(w) \leqslant n(v)$, and that equality holds for all such w exactly if v lies in U. Choosing w to be a vertex admitting a path from v to w for which the value of $n(w)$ is minimal, we see that for any vertex there is a path from that vertex to a vertex in U. An argument analogous as in the proof of Lemma 13.1.2 (but with U playing the role of the vertex v in that proof) shows that there is an input string p such that for every path with label p originating from any vertex, the end vertex lies in some strongly connected component.

We now assume that A is *sparse*, and we claim that then all vertices in U have vertex label 0. Indeed, by the combinatorial criterion in Proposition 12.1.2, A has no tied vertices, but any vertex v with label 1 lying in some strongly connected component is tied: by strong connectedness, two directed edges starting at v with different labels can each be continued to paths p and q leading back to v, and then pq and qp are two different paths of the same length connecting v to itself.

Thus, the automaton A' obtained by replacing every vertex in U with a single absorbing state with vertex label 0 produces the same output as A. We conclude that if A is *sparse and minimal*, it has only one strongly connected component, and this component is an absorbing state with label 0. □

13.2. 'Non-randomness'

A power series corresponding to a synchronising automaton with an absorbing state is not 'random' at all: if the binary expansion of n contains a synchronising word p_{sync}

leading to an absorbing state, the corresponding coefficient a_n will always be the same, namely the output value of the absorbing state. Since most integers have binary expansions containing p_{sync}, it follows that a_n is constant for 'almost all' n, i.e. there is some $c > 0$ such that a_n takes the same value for all except $O(N^{1-c})$ values $n < N$.

So far, we used the convention that our automata were leading-zero invariant, which we now drop. In order to produce automatic sequences from automata, we used the backwards-reading convention (starting from the least significant digit), and sequences obtained in this manner from synchronising automata may be more properly called *backwards synchronising* to distinguish them from the forwards-reading convention (starting from the most significant digit), which leads to the notion of a *forwards synchronising* automatic sequence. For a given sequence, these two notions are not equivalent (the sequence (n mod 2) is forwards synchronising, but not backwards synchronising, and we will see below that the sequence of coefficients of the series $\sigma_{\min}$ is backwards synchronising, but not forwards synchronising). With both of these notions at hand, we may now refer to the following precise result about structured versus random sequences. In [19, Thm. C] it was shown that any $\mathbf{C}$-valued automatic sequence (such as our sequences with the output alphabet $\mathbf{F}_2$ lifted to $\{0,1\} \subset \mathbf{C}$) can be decomposed as a sum of a 'structured sequence', in which the n-th coefficient is a function of the n-th coefficients of a periodic sequence and forwards and backwards synchronising sequences, and a 'random sequence', meaning a highly Gowers uniform sequence. (Since in this sense sequences that are 0 almost everywhere are 'random', the terminology is somewhat loose.) The classical Thue–Morse sequence is an example of a highly Gowers uniform sequence [49]. By contrast, it turns out that our sequences are very structured and non-random in the sense of this decomposition. As an example, consider the series σ_{CS}: it follows from Equation (12) that the value of its n-th coefficient for $n \geqslant 3$ depends only on the two leading digits and the final digit of the base-2 expansion of n.

Proposition 13.2.1. *For all series $\sigma = \sum a_n t^n$ in Table 9 the sequence (a_n) is* structured: *there exists a backwards synchronising sequence (b_n), a forwards synchronising sequence (f_n) and a function $F\colon \mathbf{F}_2^2 \to \mathbf{F}_2$ such that $a_n = F(b_n, f_n)$ for all n.*

Proof. All series in Table 9 except $\sigma_{\min}$, $\sigma_{\text{CS}}^{\circ 2}$, σ_{CS}, σ_{J} and $\sigma_{\text{J}}^{\circ 3}$ are produced by automata that admit an absorbing state that is accessible from any other state of the automaton, and hence by Lemma 13.1.2, they are (backwards and forwards) synchronising. Indeed, for small automata, one may inspect the pictures; for the larger automata, the verification can be found in [17]; for the series $\sigma_{\text{S},2^\mu+1}$, for which we have not given a representation of the corresponding automata, one may rely on their sparseness and invoke Lemma 13.1.3.

To treat the remaining cases, we observe the following. The minimal automaton corresponding (in backwards-reading convention) to $\sigma_{\min}$ is synchronising with synchronising word 1^3, and so the corresponding sequence is backwards synchronising (using [19, Lemma 3.2] it can be proven that it is not forwards synchronising). The automata

corresponding to σ_{J} and $\sigma_{\mathrm{J}}^{\circ 3}$ have two absorbing states, and every state has a path to one of these two states; this is enough to conclude that these sequences are forwards synchronising (cf. [19, Lemma 3.2]). Finally, the automata for $\sigma_{\mathrm{CS}}^{\circ 2}$ and σ_{CS} have two subgraphs that are synchronising and the start vertex is connected by an outgoing edge to these two subgraphs; it follows that the value a_n of the corresponding sequence depends on the value of a backwards synchronising sequence (the sequence produced by the product automaton for the subgraphs) and on the value of the sequence (n mod 2), which is forwards synchronising. □

Synchronisability is not invariant under conjugation of the corresponding power series, so one may wonder whether every conjugacy class of elements of finite order in $\mathscr{N}(\mathbf{F}_2)$ has a synchronising representative.

How computations and visualisations were done

- Equations and uniformisers were computed by hand. Singular or Mathematica were used for elimination of variables and checking irreducibility of equations.
- Automata were generated in Mathematica by Rowland's package [58]. Shapes of automata were verified using the Magma code in [14]. This code was also used to compute the number of states of certain automata that were not computed in further detail.
- Automata were redrawn using tikz and Evan Walace's Finite State Machine Design app (`github.com/evanw/fsm`), with the exception of the visualisation of the automaton for $\sigma_{(1,9)}$, which was drawn in Mathematica, exported as eps and the 'Start'-label was added in Inkskape.
- The genus of the curves in Table 7 were computed using Singular, with the exception of $\sigma_{(1,9)}$, which was computed in Magma.
- All claimed automata and explicit series representations were verified in Mathematica to $O(t^{200})$ at least.
- The file `LabelledDirectedGraph.txt` in [14] contains the Magma-routine to compute the labelled directed graph structure (without vertex output labels) from Algorithm 3.1.2 using the method of differential forms, in a form that can be parsed by Rowland's Mathematica package [58]. We give two examples of the running time using the online calculator for Magma V2.25-5: for $\sigma_{\min}$ the labelled directed graph is computed in 0.090 seconds, and the computation of the number of states in Remark 7.3 being 668 required 2.74 seconds.

Description of supplementary material

- The file `automata-of-finite-order` contains, for each of the series occurring in this paper, an irreducible algebraic equation that it satisfies, initial coefficients that uniquely determine it as a solution to that algebraic equation, and the corresponding

automaton, stored in the format of [58] and visualised as a graph. The series occur by the name used in the current paper, and are ordered by compositional order, then by lexicographical order of the lower break sequence.

- The file `verification-of-non-sparseness` contains the material needed to verify combinatorially that $\sigma_{(1,9)} \notin \widehat{S}$.
- The file `verification-of-synchronisation` contains the material needed to verify that $\sigma_{V,3}$, $\sigma_{(1,9)}$ and σ_8 are synchronising.

Acknowledgments

JB was supported by National Science Center, Poland under grant no. 2016/23/-D/ST1/01124. DT was supported in part by the research training group *GRK 2240: Algebro-geometric Methods in Algebra, Arithmetic and Topology*, funded by the DFG.

We thank Jeroen Sijsling for advice on various computations, Jonathan Lubin for sharing his unpublished work on conjugacy classes in the Nottingham group, Andrew Bridy and Eric Rowland for many interesting discussions about implementations, and Jason Bell for some insightful discussions. We also thank Ragnar Groot Koerkamp for setting up a computer search for small automata. We also thank the reviewer for some pertinent suggestions that are reflected in Subsection 8.3 and Remark 12.2.3.

Appendix A. Supplementary material

Supplementary material related to this article can be found online at https://doi.org/10.1016/j.jalgebra.2022.03.019.

References

[1] Boris Adamczewski, Jason P. Bell, On vanishing coefficients of algebraic power series over fields of positive characteristic, Invent. Math. 187 (2) (2012) 343–393.
[2] Boris Adamczewski, Jason P. Bell, Diagonalization and rationalization of algebraic Laurent series, Ann. Sci. Éc. Norm. Supér. (4) 46 (6) (2013) 963–1004.
[3] Boris Adamczewski, Reem Yassawi, A note on Christol's theorem, arxiv:1906.08703, 2019 (14 pp.), not for publication.
[4] Seda Albayrak, Jason P. Bell, A refinement of Christol's theorem for algebraic power series, Math. Z. 300 (3) (2022) 2265–2288.
[5] Jean-Paul Allouche, Jeffrey Shallit, Automatic Sequences, Cambridge University Press, Cambridge, 2003.
[6] Laurent Bartholdi, Endomorphic presentations of branch groups, J. Algebra 268 (2) (2003) 419–443.
[7] Mikhail V. Berlinkov, On the probability of being synchronizable, in: Algorithms and Discrete Applied Mathematics, in: Lecture Notes in Comput. Sci., vol. 9602, Springer, Cham, 2016, pp. 73–84.
[8] José Bertin, Ariane Mézard, Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques, Invent. Math. 141 (1) (2000) 195–238.
[9] Frauke M. Bleher, Ted Chinburg, Bjorn Poonen, Peter Symonds, Automorphisms of Harbater-Katz-Gabber curves, Math. Ann. 368 (1–2) (2017) 811–836.
[10] Svetlana I. Bogataya, Semen A. Bogatyi, Denis D. Kiselev, Powers of elements of the series substitution group $\mathscr{J}(\mathbb{Z}_2)$, Topol. Appl. 201 (2016) 29–56.
[11] Wieb Bosma, John Cannon, Catherine Playoust, The Magma algebra system. I. The user language, in: Computational Algebra and Number Theory (London, 1993), J. Symb. Comput. 24 (3–4) (1997) 235–265, http://magma.maths.usyd.edu.au/magma/.

[12] Alin Bostan, Xavier Caruso, Gilles Christol, Philippe Dumas, Fast coefficient computation for algebraic power series in positive characteristic, in: R. Scheidler, J. Sorenson (Eds.), ANTS XIII – Proceedings of the Thirteenth Algorithmic Number Theory Symposium, U Wisconsin, Madison, in: The Open Book Series, vol. 2, Mathematical Sciences Publishers, Berkeley, 2019, pp. 119–135, http://msp.org/obs/2.
[13] Andrew Bridy, Automatic sequences and curves over finite fields, Algebra Number Theory 11 (3) (2017) 685–712.
[14] Andrew Bridy, Gunther Cornelissen, `LabelledDirectedGraph.txt`, MAGMA routine, supplementary material, https://arxiv.org/abs/2008.04971, 2020.
[15] Jakub Byszewski, Gunther Cornelissen, Which weakly ramified group actions admit a universal formal deformation?, Ann. Inst. Fourier (Grenoble) 59 (3) (2009) 877–902.
[16] Jakub Byszewski, Gunther Cornelissen, Fumiharu Kato, Un anneau de déformation universel en conducteur supérieur, Proc. Jpn. Acad., Ser. A, Math. Sci. 88 (2) (2012) 25–27.
[17] Jakub Byszewski, Gunther Cornelissen, Djurre Tijsma, `automata-of-finite-order`; `verification-of-non-sparseness`; `verification-of-synchronisation`, MATHEMATICA® (v12) notebooks (nb) and pdf printout (pdf), supplementary material, https://arxiv.org/abs/2008.04971, 2020.
[18] Jakub Byszewski, Jakub Konieczny, Automatic sequences and generalised polynomials, Can. J. Math. 72 (2) (2020) 392–426.
[19] Jakub Byszewski, Jakub Konieczny, Clemens Müllner, Gowers norms for automatic sequences, preprint, arXiv:2002.09509, 2020.
[20] Rachel Camina, Subgroups of the Nottingham group, J. Algebra 196 (1) (1997) 101–113.
[21] Rachel Camina, The Nottingham group, in: Marcus du Sautoy, Dan Segal, Aner Shalev (Eds.), New Horizons in Pro-p Groups, in: Progr. Math., vol. 184, Birkhäuser Boston, Boston, MA, 2000, pp. 205–221.
[22] Ted Chinburg, Peter Symonds, An element of order 4 in the Nottingham group at the prime 2, preprint, arXiv:1009.5135, 2010, 3 pp.
[23] Gilles Christol, Ensembles presque periodiques k-reconnaissables, Theor. Comput. Sci. 9 (1) (1979) 141–145.
[24] Gilles Christol, Teturo Kamae, Michel Mendès France, Gérard Rauzy, Suites algébriques, automates et substitutions, Bull. Soc. Math. Fr. 108 (4) (1980) 401–419.
[25] Alan Cobham, On the base-dependence of sets of numbers recognizable by finite automata, Math. Syst. Theory 3 (1969) 186–192.
[26] Alan Cobham, Uniform tag sequences, Math. Syst. Theory 6 (1972) 164–192.
[27] Keith Conrad, Galois groups of cubics and quartics in all characteristics, https://kconrad.math.uconn.edu/blurbs/galoistheory/cubicquarticallchar.pdf. (Accessed 4 November 2019), undated expository note (21 pp.).
[28] Gunther Cornelissen, Fumiharu Kato, Equivariant deformation of Mumford curves and of ordinary curves in positive characteristic, Duke Math. J. 116 (3) (2003) 431–470.
[29] Gunther Cornelissen, Fumiharu Kato, Zur Entartung schwach verzweigter Gruppenoperationen auf Kurven, J. Reine Angew. Math. 589 (2005) 201–236.
[30] Gunther Cornelissen, Ariane Mézard, Relèvements des revêtements de courbes faiblement ramifiés, Math. Z. 254 (2) (2006) 239–255.
[31] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, Hans Schönemann, SINGULAR 4-1-2 — A computer algebra system for polynomial computations, http://www.singular.uni-kl.de, 2019 (used through Singular Online, 11 July 2019).
[32] Mikhail Ershov, On the commensurator of the Nottingham group, Trans. Am. Math. Soc. 362 (12) (2010) 6663–6678.
[33] Ivan B. Fesenko, On just infinite pro-p-groups and arithmetically profinite extensions of local fields, J. Reine Angew. Math. 517 (1999) 61–80.
[34] Ivan B. Fesenko, Sergei V. Vostokov, Local Fields and Their Extensions, second ed., Translations of Mathematical Monographs, vol. 121, American Mathematical Society, Providence, RI, 2002.
[35] Harry (Hillel) Furstenberg, Algebraic functions over finite fields, J. Algebra 7 (1967) 271–277.
[36] Barry Green, Realizing deformations of curves using Lubin-Tate formal groups, Isr. J. Math. 139 (2004) 139–148.
[37] Ragnar Groot Koerkamp, C++ program for searching small automata for algebraic power series over $\mathbf{F}_2$, https://github.com/RagnarGrootKoerkamp/automata/releases/tag/v1.0 (version released 5 Aug 2020).
[38] David Harbater, Moduli of p-covers of curves, Commun. Algebra 8 (12) (1980) 1095–1122.

[39] David R. Hayes, Explicit class field theory for rational function fields, Trans. Am. Math. Soc. 189 (1974) 77–91.
[40] Juka Honkala, A decision method for the recognizability of sets defined by number systems, RAIRO Inform. Théor. Appl. 20 (4) (1986) 395–403.
[41] Chun Yin Hui, Krishna Kishore, Torsion elements of order p^2 in the Nottingham group, J. Group Theory 23 (3) (2020) 489–502.
[42] Sandrine Jean, Classification à conjugaison près des séries de p-torsion, Doctoral Thesis (108 pp.), Université de Limoges, https://www.theses.fr/2008LIMO4011, 2008. (Accessed 6 April 2018).
[43] Sandrine Jean, Conjugacy classes of series in positive characteristic and Witt vectors, J. Théor. Nr. Bordx. 21 (2) (2009) 263–284.
[44] Stephen A. Jennings, Substitution groups of formal power series, Can. J. Math. 6 (1954) 325–340.
[45] Kiyomi Kanesaka, Koji Sekiguchi, Representation of Witt vectors by formal power series and its applications, Tokyo J. Math. 2 (2) (1979) 349–370.
[46] Nicholas M. Katz, Local-to-global extensions of representations of fundamental groups, Ann. Inst. Fourier 36 (4) (1986) 69–106.
[47] Denis D. Kiselev, Explicit embeddings of finite abelian p-groups in the group $\mathscr{J}(\mathbb{F}_p)$, Mat. Zametki 97 (1) (2015) 74–79.
[48] Benjamin Klopsch, Automorphisms of the Nottingham group, J. Algebra 223 (1) (2000) 37–56.
[49] Jakub Konieczny, Gowers norms for the Thue-Morse and Rudin-Shapiro sequences, Ann. Inst. Fourier (Grenoble) 69 (4) (2019) 1897–1913.
[50] Aristides Kontogeorgis, Ioannis Tsouknidas, A cohomological treatise of HKG-covers with applications to the Nottingham group, J. Algebra 555 (2020) 325–345.
[51] Peter Linz, An Introduction to Formal Languages and Automata, 6th edition, Jones and Bartlett Publishers, 2016.
[52] Falko Lorenz, Algebra. Vol. II (Fields with Structure, Algebras and Advanced Topics), Universitext, Springer, New York, 2008.
[53] Jonathan Lubin, Classifying torsion elements of the Nottingham group of period p^2 and type $\langle 1, m\rangle$, unpublished manuscript (9 pp.), 23 Jan 2016.
[54] Jonathan Lubin, Torsion in the Nottingham group, Bull. Lond. Math. Soc. 43 (3) (2011) 547–560.
[55] Jonathan Lubin, John Tate, Formal complex multiplication in local fields, Ann. Math. (2) 81 (1965) 380–387.
[56] Barry Mazur, An introduction to the deformation theory of Galois representations, in: Modular Forms and Fermat's Last Theorem, Boston, MA, 1995, Springer, New York, 1997, pp. 243–311.
[57] R. Hjalmar Mellin, Résolution de l'équation algébrique générale à l'aide de la fonction gamma, C. R. Acad. Sci., Paris 172 (1921) 658–661.
[58] Eric Rowland, IntegerSequences, a MATHEMATICA® package for identifying and analyzing a variety of classes of integer sequences, https://github.com/ericrowland/IntegerSequences (version 1.53 dated 30 May 2020).
[59] Eric Rowland, IntegerSequences: a package for computing with k-regular sequences, in: J.H. Davenport, M. Kauers, G. Labahn, J. Urban (Eds.), 6th International Congress on Mathematical Software – ICMS 2018, South Bend, in: Lecture Notes in Computer Science, vol. 10931, Springer, Cham, 2018, pp. 414–421.
[60] Eric Rowland, Reem Yassawi, Automatic congruences for diagonals of rational functions, J. Théor. Nr. Bordx. 27 (1) (2015) 245–288.
[61] Imke Rust, Ortwin Scheja, A guide to explicit class field theory in global function fields, in: Drinfeld Modules, Modular Schemes and Applications, Alden-Biesen, 1996, World Sci. Publ., River Edge, NJ, 1997, pp. 44–65.
[62] Henning Stichtenoth, Algebraic Function Fields and Codes, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.
[63] Andrew Szilard, Sheng Yu, Kaizhong Zhang, Jeffrey Shallit, Characterizing regular languages with polynomial densities, in: Mathematical Foundations of Computer Science 1992, Prague, 1992, in: Lecture Notes in Comput. Sci., vol. 629, Springer, Berlin, 1992, pp. 494–503.
[64] Djurre Tijsma, Automata and finite order elements in the Nottingham group, Master thesis, Utrecht University, 2018.
[65] Bradley Weaver, The local lifting problem for D_4, Isr. J. Math. 228 (2) (2018) 587–626.

Chapter 4

Commensurability zeta function

In this chapter we study a new type of arithmetic function associated to a group, the commensurability function, introduced recently in 2020 by Bou-Rabee and Studenmund in [8] for unipotent algebraic $\mathbf{Z}$-groups. For these types of groups the two authors show that the associated commensurability zeta function admits an Euler product and that the local factors are rational. Making the commensurability function an interesting object to study. We expand the list of known commensurability zeta functions by including an infinite family of abelian groups, for this family we show a connection to the subgroup zeta function, and we generalise the commensurability function to the setting of modules.

In the first section we give an introduction to the commensurability (zeta) function for groups and generalise this to the setting of modules. We state the theorems we prove in this chapter and we also give an outlook to possible further research in this area.

The second section covers some preliminary results such as R-lattices. The third section is concerned with a proof of the Euler product of the commensurability zeta function for modules. In the final section we put everything together and provide a proof of the formula for the commensurability zeta function for a family of abelian groups.

The appendix covers two alternative methods to compute commensurability zeta functions in some low dimensional cases, which are already covered by one of the main theorems of this chapter. The first method uses a standard basis for 2×2-matrices over a non-Archimedean local field and the second method makes use of the theory of buildings of $\mathrm{GL}_d(\mathbf{Q}_p)$. These alternative proofs could provide inspiration to compute other commensurability zeta functions.

4.1 Introduction

4.1.1 Commensurability function for groups

Let G be a group and let $H, K \leq G$ be two subgroups of G. We say that the groups H and K are *commensurable* (in the strict sense as subgroups of G), if their *commensurability index*

$$c(H,K) = |H : H \cap K| \cdot |K : H \cap K|$$

is finite. This is a generalisation of the notion of commensurability for real numbers, two non-zero real numbers are said to be commensurable if their ratio is a rational number. Clearly, every two subgroups of a finite group are commensurable. Examples of two non-commensurable subgroups of a group are also easy to be found. For example, take any infinite group and consider two subgroups, one which is finite and one that is infinite. Fixing a subgroup $K \leq G$, we consider the *commensurability function*

$$c^{G,K} : \mathbf{N} \to \mathbf{N} \cup \{0, \infty\}, \quad n \mapsto c_n^{G,K},$$

where

$$c_n^{G,K} = |\{H \leq G \mid c(H,K) = n\}|,$$

i.e. the number of subgroups of G having commensurability index n with K. In case the commensurability function $c^{G,K} : \mathbf{N} \to \mathbf{N} \cup \{0, \infty\}$ takes on only finite values, we associate to the pair (G,K) the *commensurability zeta function for the pair* (G,K), denoted by $\zeta_{G,K}^{\mathrm{comm}}(s)$, which is the (formal) Dirichlet series

$$\zeta_{G,K}^{\mathrm{comm}}(s) = \sum_{n=1}^{\infty} c_n^{G,K} n^{-s}, \quad s \in \mathbf{C}.$$

The abscissa of convergence of the zeta function $\zeta_{G,K}^{\mathrm{comm}}(s)$ is related to the growth type of the *commensurability growth function* $s^{G,K}$, which is defined by

$$s^{G,K} : \mathbf{N} \to \mathbf{N}, \quad n \mapsto s_n^{G,K} = \sum_{k=1}^{n} c_k^{G,K}.$$

In the following we study properties of the commensurability zeta function, for instance how the algebraic properties of the groups G, K control the analytic properties of $\zeta_{G,K}^{\mathrm{comm}}(s)$ and vice versa. This is similar to other zeta functions counting other substructures such as the (normal, subnormal, maximal) finite-index subgroups or the finite dimensional representations over $\mathbf{C}$; for some examples see [63]. We do have an additional degree of flexibility, since we consider a pair (G,K) of groups instead of a single group G.

Choosing $K = G$ in the definition of the commensurability function, we recover the well-known function

$$\mathbf{N} \to \mathbf{N} \cup \{0, \infty\}, \quad n \mapsto a_n(G) = |\{H \leq G \mid |G : H| = n\}|,$$

counting the number of subgroups of finite index in G. This gives rise to the subgroup growth function $n \mapsto \sum_{k=1}^{n} a_k(G)$ and the subgroup zeta function $\zeta_{G,G}^{\mathrm{comm}}(s) = \zeta_G^{\leq}(s)$ in case $a_n(G)$ is finite for every $n \in \mathbf{N}$. In 1949 Hall computed $a_n(F_g)$ for the free group F_g on g generators [29], hereby starting the investigation into the subgroup growth of groups. However, only after the influential 1988 paper [27] by Grunewald, Segal and Smith, concerning the subgroup growth of nilpotent groups, this area gained significant attention. One of the greatest achievements is the characterisation of the groups with polynomial subgroup growth as the virtually solvable groups of finite rank in 1993 by Lubotzky, Mann and Segal [42].

The commensurability function is a new type of arithmetic function for groups introduced in 2020 by Bou-Rabee and Studenmund [8]. The commensurability growth function is a generalisation of the subgroup growth function and it is an interesting question, which results from the area of subgroup growth can be generalised to the setting of the commensurability function. In [8] it is shown that there are some parallels between the two worlds. Besides generalising the subgroup growth function, the commensurability function is also an upper bound for the subgroup growth function. Namely, for a group G and a subgroup $K \leq G$ we have for every $n \in \mathbf{N}$ that $a_n(K) \leq c_n^{G,K}$. More generally, if $|G : K| < \infty$, then the subgroups $H \leq G$, which are commensurable with K, are precisely the finite index subgroups of G. The full impact of these relationships is yet to be explored. There are other cases where we do find something interesting.

In [8] the commensurability function is studied for the class of unipotent algebraic $\mathbf{Z}$-groups; e.g. algebraic group defined over $\mathbf{Z}$, see also [52]. For every unipotent algebraic $\mathbf{Z}$-group G Bou-Rabee and Studenmund prove that the commensurability function of its real Lie group $G(\mathbf{R})$, with respect to the arithmetic lattice $G(\mathbf{Z})$, takes only finite values. Therefore the corresponding commensurability zeta function of the pair $(G(\mathbf{R}), G(\mathbf{Z}))$ is defined. They show that the zeta function $\zeta_{G(\mathbf{R}),G(\mathbf{Z})}^{\mathrm{comm}}(s)$ admits the formal Euler product

$$\zeta_{G(\mathbf{R}),G(\mathbf{Z})}^{\mathrm{comm}}(s) = \prod_p \zeta_{G(\mathbf{R}),G(\mathbf{Z})}^{\mathrm{comm},p}(s), \tag{4.1}$$

where p runs over all prime numbers, the functions

$$\zeta_{G(\mathbf{R}),G(\mathbf{Z})}^{\mathrm{comm},p}(s) = \sum_{n=0}^{\infty} c_{p^n}^{G(\mathbf{R}),G(\mathbf{Z})} p^{-ns}$$

are called the local factors. The local factors enumerate the subgroups of G whose commensurability index with K is a power p. Using techniques from model theory and p-adic

integration [46], previously succesfully applied to the area of subgroup growth (see [45, Chapter 15 and Window 12]), they prove that the local factors $\zeta^{\mathrm{comm},p}_{G(\mathbf{R}),G(\mathbf{Z})}(s)$ are rational functions over $\mathbf{Q}$ in p^{-s}. Moreover, there are bounds on the degree of the numerator and denominator of these rational functions, that are independent of the prime number p. This mirrors a similar behaviour of the zeta functions related to subgroup growth and representation growth; see [27, 30].

The only example, of an explicitly computed commensurability zeta function for a pair of different groups, known to Bou-Rabee and Studenmund, is the commensurability zeta function for the pair $(\mathbf{R}, \mathbf{Z})$ of abelian groups [8, Prop. 2.1], which they compute as

$$\zeta^{\mathrm{comm}}_{\mathbf{R},\mathbf{Z}}(s) = \frac{\zeta(s)^2}{\zeta(2s)} = \sum_{n=1}^{\infty} \frac{2^{\omega(n)}}{n^s},$$

where $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is the ordinary Riemann zeta function and $\omega(n)$ counts the number of different prime factors of n. Any subgroup of $\mathbf{R}$, which is commensurable with $\mathbf{Z}$, is actually a subgroup of $\mathbf{Q}$, so in fact $\zeta^{\mathrm{comm}}_{\mathbf{R},\mathbf{Z}}(s) = \zeta^{\mathrm{comm}}_{\mathbf{Q},\mathbf{Z}}(s)$. In [9] Bou-Rabee, Kaletha and Studenmund compute some asymptotics of the commensurability growth function $s^{G,\Gamma}$ for a Chevalley group scheme G defined over $\mathbf{Z}$ of rank greater than 1 and an arithmetic lattice Γ in $G(\mathbf{R})$. They show that the asymptotic behaviour of $s^{G,\Gamma}$ depends on the subgroup growth function $n \mapsto \sum_{k=1}^{n} a_k(\Gamma)$ of Γ and a constant depending only on the root system of G.

Our contribution to the study of the commensurability function is the explicit computation of the commensurability zeta functions for an infinite family of pairs of groups. This extends the current list of known examples from a single one to infinitely many. Not only does this give more examples to test hypotheses on, it also shows an interesting and unexpected connection to the theory of subgroup growth, as we can express the commensurability zeta function completely in terms of a subgroup zeta function.
We compute for any positive integer $d \in \mathbf{N}$ for the pair $(\mathbf{R}^d, \mathbf{Z}^d)$ of abelian groups the commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{R}^d,\mathbf{Z}^d}(s) = \zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$; see Theorem 4.1.1. In the wording of [8] this covers the case where G is an abelian unipotent connected algebraic group defined over $\mathbf{Z}$. Because G is defined over $\mathbf{Z}$, G is $\mathbf{Q}$-isomorphic to a $\mathbf{Q}$-vector group H (see [33, Appendix A.3]), so that $G(\mathbf{R}) \cong H(\mathbf{R}) \cong \mathbf{R}^d$ for some $d \in \mathbf{N}$. Under this $\mathbf{Q}$-isomorphism the image of $G(\mathbf{Z})$ is commensurable with $H(\mathbf{Z})$ [52, Prop. 4.1], which is a lattice of full rank in $H(\mathbf{R})$. Any two lattices of full rank inside $\mathbf{R}^d$ have the same commensurability zeta function and since any lattice of full rank in $\mathbf{R}^d$ which is commensurable with $\mathbf{Z}^d$ lies in $\mathbf{Q}^d$, we can reduce our computation to the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ of abelian groups.

The next theorem shows that the commensurability zeta function for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ is related to the subgroup zeta function of $\mathbf{Z}^d$. Actually, this theorem is obtained as a corollary of a more general statement, see Theorem 4.1.5, which deals with a generalisation of the commensurability function of pairs of abelian groups to modules.

Theorem 4.1.1. *Let $d > 0$ be an integer. The commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ of abelian groups satisfies*

$$\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s) \cdot \zeta^{\leq}_{\mathbf{Z}^d}(2s) = \zeta^{\leq}_{\mathbf{Z}^d}(s)^2, \tag{4.2}$$

where $\zeta^{\leq}_{\mathbf{Z}^d}(s)$ denotes the subgroup zeta function of $\mathbf{Z}^d$.

The proof of Theorem 4.1.1 not only shows that the commensurability zeta function satisfies equation (4.2), but actually explains the connection between the commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ and the subgroup zeta function $\zeta^{\leq}_{\mathbf{Z}^d}(s)$. Therefore the equation (4.2) is more than a coincidence of Dirichlet series. Two alternative proofs for Theorem 4.1.1 are given in the appendix for the cases $d \in \{2, 3\}$; one proof uses a standard basis for lattices and the other proof makes use of a Bruhat-Tits building. It is a well-known result, see [45, Chapter 15] for multiple proofs, that the subgroup zeta function for $\mathbf{Z}^d$ is given by

$$\zeta^{\leq}_{\mathbf{Z}^d}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1),$$

where $\zeta(s)$ is the ordinary Riemann zeta function. Consequently, by using Theorem 2.0.3, we have the following corollary of Theorem 4.1.1, describing the commensurability growth.

Corollary 4.1.2. *Let $d > 0$ be an integer. The commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ is given by the formula*

$$\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s) = \prod_{k=0}^{d-1} \frac{\zeta(s-k)^2}{\zeta(2s-k)}$$

and hence the commensurability growth $n \mapsto s_n^{\mathbf{Q}^d,\mathbf{Z}^d}$ of the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ satisfies

$$s_n^{\mathbf{Q}^d,\mathbf{Z}^d} \sim \frac{C}{d} n^d \log(n) \quad \text{as} \quad n \to \infty,$$

where the constant C is given by

$$C = \frac{\zeta(2)^2\zeta(3)^2\cdots\zeta(d)^2}{\zeta(d+1)\zeta(d+2)\cdots\zeta(2d)}.$$

4.1.2 Commensurability function for modules

We consider a generalisation of the commensurability zeta function for groups discussed in the previous section to modules. This is largely analogous with the group-theoretical version in the previous chapter. Let R be a ring (commutative with 1) and let M be an

R-module. For two R-submodules Λ, Γ of M we define the *commensurability index* $c(\Lambda, \Gamma)$ by

$$c(\Lambda, \Gamma) = |\Lambda : \Lambda \cap \Gamma| \cdot |\Gamma : \Lambda \cap \Gamma|,$$

here $|- : -|$ denotes the index of the underlying abelian groups. When $c(\Lambda, \Gamma)$ is finite, we say that Λ and Γ are *commensurable* (in the strict sense as submodules of M). Fixing an R-submodule $N \subseteq M$, the *commensurability function* $c^{M,N} : \mathbf{N} \to \mathbf{N} \cup \{\infty\}, n \mapsto c_n^{M,N}$ is defined by

$$c_n^{M,N} = |\{\Lambda \subseteq M \mid \Lambda \text{ an } R\text{-submodule}, c(\Lambda, N) = n\}|.$$

The *commensurability zeta function* for the pair (M, N) of R-modules is defined by the (formal) Dirichlet series

$$\zeta_{M,N}^{\mathrm{comm}}(s) = \sum_{n=1}^{\infty} c_n^{M,N} n^{-s}, \quad s \in \mathbf{C}.$$

The *submodule zeta function* $\zeta_N^{\mathrm{sub}}(s)$, corresponding to the R-module N, is the formal series

$$\zeta_N^{\mathrm{sub}}(s) = \sum_{\Lambda \subseteq N} |N : \Lambda|^{-s}, \quad s \in \mathbf{C},$$

where we sum over all R-submodules $\Lambda \subseteq N$ of finite index in N. Since $\Lambda \subseteq N$ we have $c(\Lambda, N) = |N : \Lambda|$. This zeta function $\zeta_N^{\mathrm{sub}}(s)$ is a generalisation of the subgroup zeta function or the ideal zeta function to modules; see also [12], [39], [56] and [57].

We will turn our attention to the case $(M, N) = (K^d, R^d)$ with R an integral domain with field of fractions K and $d \in \mathbf{N}$. An *R-lattice* in K^d is a finitely generated R-submodule of K^d containing a basis of K^d; see [51, §81] for more on R-lattices. Other names for R-lattices can be found in the literature, such as full-rank lattice or K-lattice. We write $\mathcal{L}(R^d), \mathcal{L}(K^d)$ for the set of all R-lattices in K^d contained in R^d, K^d respectively.

When K is a global field or a non-Archimedean local field (see also Chapter 2) the set $\mathcal{L}(K^d)$ coincides with the set of all R-submodules of K^d which are commensurable with R^d. This turns out to be very helpful. The next theorem describes necessary and sufficient conditions on the ring R for this to hold.

Theorem 4.1.3. *Let R be an integral domain with fraction field K, let $d \in \mathbf{N}$ and let $\Lambda \subseteq K^d$ be a non-zero R-submodule. The ring R satisfies the two conditions*

(1) if $d > 1$, then R is infinite;

(2) for every non-zero ideal $I \subseteq R$ we have $|R : I| < \infty$,

if and only if we have the equivalence

$$\Lambda \in \mathcal{L}(K^d) \Leftrightarrow c(\Lambda, R^d) < \infty. \tag{4.3}$$

The ring $R = \mathbf{Z} + 2\mathbf{Z}\sqrt{2}$ is an example of a ring for which condition (2) holds, which is not the ring of integers of a global field or a non-Archimedean local field.

Every pair (M, N) of R-modules with $N \subseteq M$ can also be considered as a pair of abelian groups by forgetting the R-module structure. One expects that this in general leads to different commensurability zeta functions. When $R = \mathbf{Z}$ the modules M, N are just abelian groups and hence the commensurability zeta functions, when considered as abstract groups or as modules, coincide. This applies to the pairs $(\mathbf{Q}^d, \mathbf{Z}^d)$ with $d \in \mathbf{N}$. Let K be a number field with $d = [K : \mathbf{Q}] > 1$ and let $\mathcal{O}$ the ring of integers of K. We show in Example 4.2.19 that the pair $(K, \mathcal{O})$ as $\mathcal{O}$-modules and the pair $(K, \mathcal{O})$ as abelian groups, i.e. $K \cong \mathbf{Q}^d$ and $\mathcal{O} \cong \mathbf{Z}^d$, have different commensurability zeta functions. Because our notation for the commensurability (zeta) function does not distinguish between groups and modules, it is important to stress which one is being used. For the remainder of this chapter we only work with the commensurability zeta function for modules, unless explicitly stated otherwise.

A key step in the proof of Theorem 4.1.5, the analogue of Theorem 4.1.1 for global fields, is the reduction to non-Archimedean local fields. This reduction is achieved through the existence of an Euler product for the commensurability zeta function; this is the content of the next theorem. Its proof is an adaptation and a generalisation of [8, Prop. 1.2] to the setting of modules with the Chinese remainder theorem for modules as its key step.

Theorem 4.1.4. *Let $d > 0$ be an integer and let K be a global field with ring of integers $\mathcal{O}$. The commensurability zeta function $\zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s)$ for the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules satisfies the (formal) Euler product*

$$\zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s) = \prod_{\mathfrak{p}} \zeta^{\mathrm{comm}}_{K^d_{\mathfrak{p}},\mathcal{O}^d_{\mathfrak{p}}}(s),$$

where the product runs over all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$.

A similar Euler product holds for the submodule zeta function $\zeta^{\mathrm{sub}}_{\mathcal{O}^d}(s)$. The main theorem we prove in this chapter is the next theorem, which is a generalisation of Theorem 4.1.1 to modules. The key insights for the proof for non-Archimedean local fields K with ring of integers $\mathcal{O}$ is a counting argument (see Proposition 4.4.2) and averaging over all so-called '*frames*' by integrating over the profinite group $\mathrm{GL}_d(\mathcal{O})$.

Theorem 4.1.5. *Let $d > 0$ be an integer and let K be a global field or a non-Archimedean local field with ring of integers $\mathcal{O}$. The commensurability zeta function $\zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s)$ for the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules satisfies*

$$\zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s) \cdot \zeta^{\mathrm{sub}}_{\mathcal{O}^d}(2s) = \zeta^{\mathrm{sub}}_{\mathcal{O}^d}(s)^2.$$

Similar to Theorem 4.1.1, where we expressed the commensurability zeta function for the pair $(\mathbf{Q}^d, \mathbf{Z}^d)$ of groups in terms of the subgroup zeta function for $\mathbf{Z}^d$, the commensurability zeta function for the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules is expressed in terms of the

submodule zeta function for $\mathcal{O}^d$. It is interesting to note that for a non-Archimedean local field K the commensurability zeta function $\zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s)$ depends only on the inertia degree and not on the ramification degree. Together with an explicit formula for the submodule zeta function of $\mathcal{O}^d$, see Proposition 4.2.17, we have the following corollary of Theorem 4.1.5 linking the commensurability zeta function to the Dedekind zeta function ζ_K of K.

Corollary 4.1.6. *Let K be a number field with ring of integers $\mathcal{O}$ and write $\zeta_K(s)$ for the Dedekind zeta function of K. Then $\zeta_K(s)$ equals the submodule zeta function $\zeta^{\mathrm{sub}}_{\mathcal{O}}(s)$ corresponding to the $\mathcal{O}$-module $\mathcal{O}$. The commensurability zeta function for the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules is given by*

$$\zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s) = \prod_{k=0}^{d-1} \frac{\zeta_K(s-k)^2}{\zeta_K(2s-k)}.$$

Taking $K = \mathbf{Q}$ in the above corollary recovers Theorem 4.1.1.

In the setting of groups our computations cover the case of finitely generated torsion-free abelian groups. We need new ideas to compute other examples. In the light of the Euler product in [8, Prop. 1.2] it would be very interesting to know the commensurability zeta function of a non-abelian unipotent group. For example, the Heisenberg group $H(\mathbf{Q}_p)$ with respect to the subgroup $H(\mathbf{Z}_p)$ (as a subgroup of $\mathrm{GL}_3(\mathbf{Q}_p)$) with p a prime number; these two groups can be defined by

$$H(\mathbf{Q}_p) = \begin{pmatrix} 1 & \mathbf{Q}_p & \mathbf{Q}_p \\ & 1 & \mathbf{Q}_p \\ & & 1 \end{pmatrix} \quad \text{and} \quad H(\mathbf{Z}_p) = \begin{pmatrix} 1 & \mathbf{Z}_p & \mathbf{Z}_p \\ & 1 & \mathbf{Z}_p \\ & & 1 \end{pmatrix}.$$

A crucial step in the proof of Theorem 4.1.5 is equation (4.22), which, translated to the group setting, says that any subgroup of $\mathbf{Q}^d$ commensurable with $\mathbf{Z}^d$ is isomorphic to $\mathbf{Z}^d$. We do not expect this to be true for the group $H(\mathbf{Q}_p)$, but it could be interesting to define a variation on the commensurability zeta function that enumerates only subgroups which are isomorphic to $H(\mathbf{Z}_p)$.

Let K be a global field with ring of integers $\mathcal{O}$ and let S be a finite set of valuations of K, containing all Archimedean valuations of K. The ring $\mathcal{O}_S$ of S-integers in K is defined by

$$\mathcal{O}_S = \{x \in K \mid v(x) \geq 0 \text{ for all } v \in S\}.$$

Our main Theorem 4.1.5 considers pairs of $\mathcal{O}$-modules. What happens if we consider instead $\mathcal{O}_S$-modules? Do we still have an Euler product and a formula for the commensurability zeta function in terms of the submodule zeta function?

Another variation would be to consider rings of higher Krull dimensions as opposed to the ring of integers of a non-Archimedean local field. For instance local rings that are not

discrete valuation rings. An example of such a ring is the ring $\mathbf{Z}_p[\![T]\!]$ of power series in T with coefficients from the p-adic integers $\mathbf{Z}_p$ for some prime number p.

Let p be a prime number. In Section 4.5.2 of the appendix we use the theory of buildings for $\mathrm{GL}_d(\mathbf{Q}_p)$ to compute the commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(s)$ for $d \in \{2,3\}$. For other classical groups, like the symplectic group $\mathrm{Sp}_d(\mathbf{Q}_p) \leq \mathrm{GL}_{2d}(\mathbf{Q}_p)$, there exist descriptions of the corresponding building in terms of lattices. The building of $\mathrm{Sp}_d(\mathbf{Q}_p)$ is for instance contained in the building of $\mathrm{GL}_{2d}(\mathbf{Q}_p)$. Is it possible to use our approach in Section 4.5.2 to define an interesting zeta function related to the building of $\mathrm{Sp}_d(\mathbf{Q}_p)$? Another proof for the commensurability zeta function for $d = 2$ is included in Section 4.5.1, it relies on choosing a unique basis for each arithmetic lattice. We included these proofs in the appendix, because they could be a source of inspiration to tackle the computation of the commensurability zeta function for non-abelian groups.

Before proving the main results, we introduce some important definitions and notions in Section 4.2. The proof of Theorem 4.1.3, Theorem 4.1.4 and Theorem 4.1.5 can be found in Section 4.2.2, Section 4.3 and Section 4.4, respectively.

4.2 Preliminaries

In this section we introduce notation for the remainder of this chapter and we prove some basic results. We introduce $\mathcal{O}$-lattices, followed by the commensurability index and the commensurability zeta function.

4.2.1 R-lattices

Recall the definition of a lattice. For more on lattices see for instance [51, §81].

Definition 4.2.1. *Let R be an integral domain with fraction field K. An* R-lattice Λ *in K^d is a finitely generated R-submodule of K^d which contains a basis of K^d. We write $\mathcal{L}(K^d)$ for the set of all R-lattices in K^d, so*

$$\mathcal{L}(K^d) = \{\Lambda \mid \Lambda \text{ is an } R\text{-lattice in } K^d\},$$

and $\mathcal{L}(R^d) \subseteq \mathcal{L}(K^d)$ for the set of R-lattices in K^d which are contained in R^d.

In the literature our definition of an R-lattice is sometimes called a full R-lattice. For our calculations we introduce the notion of a signature matrix, which is not a standard name.

Definition 4.2.2. *Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and let π be a uniformiser for the maximal ideal of $\mathcal{O}$. We call a matrix in* $\mathrm{GL}_d(K)$ *a* signature matrix*, if it is of the form* $\mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$*, for some integers $e_i \in \mathbf{Z}$.*

For the remainder of this section we assume that K is a non-Archimedean local field with ring of integers $\mathcal{O}$. Moreover, we also fix a uniformiser π of the unique maximal ideal of $\mathcal{O}$. Because the ring of integers $\mathcal{O}$ of K is a principal ideal domain and K^d is torsion-free as an $\mathcal{O}$-module, the theory of modules over principal ideal domain shows that every $\mathcal{O}$-lattice in $\mathcal{L}(K^d)$ is free and has rank d. Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice, then there exists a basis $\{b_1, \ldots, b_d\}$ of K^d such that Λ is spanned by $b_1, \ldots, b_d$, that is

$$\Lambda = \mathcal{O}b_1 + \ldots + \mathcal{O}b_d.$$

Write B for the matrix in $\mathrm{Mat}_d(K)$ whose columns are $b_1, \ldots, b_d$ (actually $B \in \mathrm{GL}_d(K)$ since $b_1, \ldots, b_d$ form a basis of K^d). Then Λ is also given as the image of the standard lattice $\mathcal{O}^d$ under the linear map $K^d \to K^d$ induced by the matrix B. We write this as

$$\Lambda = B\mathcal{O}^d.$$

The $\mathcal{O}$-lattice Λ does not determine B uniquely, consequently there are many possibilities for B. For $B, C \in \mathrm{GL}_d(K)$ this means that from the equation $B\mathcal{O}^d = C\mathcal{O}^d$ we cannot conclude $B = C$, but only that $C = Bh$ for some matrix $h \in \mathrm{GL}_d(\mathcal{O})$.

Definition 4.2.3. *Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice and let $g \in \mathrm{GL}_d(\mathcal{O})$ be a matrix with column vectors $g_1, \ldots, g_d \in \mathcal{O}^d$. We say that the element g is a* frame *for the $\mathcal{O}$-lattice Λ, if there exist integers $e_i \in \mathbf{Z}$ for which the set*

$$\{\pi^{e_1} g_1, \ldots, \pi^{e_d} g_d\}$$

is a basis of Λ as an $\mathcal{O}$-module. Write $D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$. We say that D is a signature matrix *of Λ with respect to the frame g. Note that g being a frame for Λ is equivalent to Λ being spanned as an $\mathcal{O}$-module by the columns of the matrix gD, which is equivalent to writing*

$$\Lambda = gD\mathcal{O}^d.$$

We write $F(\Lambda)$ for the set of all frames of the $\mathcal{O}$-lattice $\Lambda \in \mathcal{L}(K^d)$, i.e.

$$F(\Lambda) = \{g \in \mathrm{GL}_d(\mathcal{O}) \mid g \text{ is a frame for } \Lambda\}.$$

Moreover if $(\Lambda, \Gamma) \in \mathcal{L}(K^d) \times \mathcal{L}(K^d)$ is a pair of $\mathcal{O}$-lattices in K^d, then we write $F(\Lambda, \Gamma)$ for the set of all simultaneous frames for Λ and Γ, i.e.

$$F(\Lambda, \Gamma) = \{g \in \mathrm{GL}_d(\mathcal{O}) \mid g \text{ is frame for both } \Lambda \text{ and } \Gamma\}.$$

Note that in the above definition we have $F(\Lambda, \mathcal{O}^d) = F(\Lambda)$. The next lemma proves that the integers $e_i \in \mathbf{Z}$ in Definition 4.2.3 are uniquely determined by g.

Lemma 4.2.4. *Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice and let $g \in F(\Lambda)$ be a frame with column vectors $g_1, \ldots, g_d \in \mathcal{O}^d$. There exist unique integers $e_1, \ldots, e_d \in \mathbf{Z}$ such that the set*

$$\{\pi^{e_1} g_1, \ldots, \pi^{e_d} g_d\}$$

is a basis of Λ.

Proof. Let $f_1, \ldots, f_d \in \mathbf{Z}$ be another set of d integers such that

$$\{\pi^{f_1} g_1, \ldots, \pi^{f_d} g_d\}$$

is a basis for the $\mathcal{O}$-module Λ. Then we can write

$$\Lambda = g \operatorname{diag}(\pi^{e_1}, \ldots, \pi^{e_d})\mathcal{O}^d = g \operatorname{diag}(\pi^{f_1}, \ldots, \pi^{f_d})\mathcal{O}^d$$

and hence there exists an $h \in \mathrm{GL}_d(\mathcal{O})$ such that

$$g \operatorname{diag}(\pi^{e_1}, \ldots, \pi^{e_d}) = g \operatorname{diag}(\pi^{f_1}, \ldots, \pi^{f_d})h.$$

This gives $h = \operatorname{diag}(\pi^{e_1 - f_1}, \ldots, \pi^{e_d - f_d})$, forcing $e_i = f_i$ for all $1 \leq i \leq d$. □

Remark 4.2.5. An $\mathcal{O}$-lattice $\Lambda \in \mathcal{L}(K^d)$ can have different signature matrices, but, as Lemma 4.2.9 will show, any two of these differ by a permutation of the diagonal entries. Moreover, Lemma 4.2.8 shows that the set $F(\Lambda)$ for any $\Lambda \in \mathcal{L}(K^d)$ is always non-empty, i.e. every $\mathcal{O}$-lattice in $\mathcal{L}(K^d)$ has a frame.

Example 4.2.6. Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice and let $h \in \mathrm{GL}_d(K)$ be a matrix whose columns are a basis for Λ. Depending on h we cannot always find integers $e_i \in \mathbf{Z}$ such that hD with $D = \operatorname{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$ is a frame for Λ. This is illustrated by the following example. Let p be a prime number and $K = \mathbf{Q}_p$ the field of p-adic rationals with ring of integers $\mathcal{O} = \mathbf{Z}_p$ and uniformiser $\pi = p$. Consider the $\mathbf{Z}_p$-lattice Λ in $\mathbf{Q}_p^2$ given by

$$\Lambda = \mathbf{Z}_p \begin{pmatrix} p \\ 1 \end{pmatrix} + \mathbf{Z}_p \begin{pmatrix} 0 \\ p^2 \end{pmatrix} = \begin{pmatrix} p & 0 \\ 1 & p^2 \end{pmatrix} \mathbf{Z}_p^2.$$

Suppose that for some integers $a, b \in \mathbf{Z}$, we have $\begin{pmatrix} p^{a+1} & 0 \\ p^a & p^{b+2} \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_p)$. Then clearly $b \geq -2$ and $a \geq 0$. But the resulting matrix has determinant $p^{a+b+3} \geq p$ and hence cannot be an element of $\mathrm{GL}_2(\mathbf{Z}_p)$. Multiplying the individual elements of a basis with scalars does not always produce a frame. An example of a frame for the $\mathbf{Z}_p$-lattice Λ is the matrix

$$\begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}_p).$$

Then Λ has as signature matrix $\operatorname{diag}(1, p^3)$ because

$$\Lambda = \begin{pmatrix} p & p^3 \\ 1 & 0 \end{pmatrix} \mathbf{Z}_p^2 = \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p^3 \end{pmatrix} \mathbf{Z}_p^2.$$

The next theorem shows that we can decompose any matrix in $\mathrm{GL}_d(K)$ in a particularly useful form. This decomposition is known in the literature under the name Cartan decomposition or KAK decomposition, see for instance [11], Proposition 4.4.3, or [38], Theorem 7.39. This decomposition is valid for a large number of fields, not just for non-Archimedean local fields. Over a non-Archimedean local field the Cartan decomposition can be proven in an elementary way, using the Gaussian elimination procedure for matrices. The Cartan decomposition is related to various other decomposition of classical groups like $\mathrm{GL}_d(K)$, for instance the Bruhat decomposition and the Iwasawa decomposition.

Theorem 4.2.7 (Cartan decomposition)**.** *Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and $d > 0$ an integer. Any matrix $A \in \mathrm{GL}_d(K)$ can be decomposed as*

$$A = BDC$$

where $B, C \in \mathrm{GL}_d(\mathcal{O})$ and $D \in \mathrm{GL}_d(K)$ is a diagonal matrix of the form

$$D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$$

for some integers $e_i \in \mathbf{Z}$ with π a uniformiser of $\mathcal{O}$. Up to a permutation of the diagonal entries, the matrix D is unique.

Lemma 4.2.8. *For any $\mathcal{O}$-lattice $\Lambda \in \mathcal{L}(K^d)$ the set $F(\Lambda)$ of frames for Λ is non-empty.*

Proof. Let $A \in \mathrm{GL}_d(K)$ be a matrix whose columns are a basis of Λ. By Theorem 4.2.7 there exist $B, C \in \mathrm{GL}_d(\mathcal{O})$ and a diagonal matrix $D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$ with $e_i \in \mathbf{Z}$ such that $A = BDC$. Because $C \in \mathrm{GL}_d(\mathcal{O})$ the columns of the matrix $AC^{-1} = BD$ form a basis of Λ, hence B is a frame for Λ. □

Lemma 4.2.9. *Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice. Any two signature matrices of Λ differ by a permutation of the diagonal entries.*

Proof. Let $g, h \in F(\Lambda)$ be two frames for Λ with corresponding signature matrices D, E. From $gD\mathcal{O}^d = hE\mathcal{O}^d$ it follows that $gDA = hE$ for some element $A \in \mathrm{GL}_d(\mathcal{O})$. The claim follows now immediately from Theorem 4.2.7. □

4.2.2 Commensurability index

Let R be a ring (commutative with 1) and M an R-module. For two R-submodules Λ, Γ of M we define the *commensurability index* $c(\Lambda, \Gamma)$ by

$$c(\Lambda, \Gamma) = |\Lambda : \Lambda \cap \Gamma| \cdot |\Gamma : \Lambda \cap \Gamma|,$$

here $|- : -|$ denotes the index of the underlying abelian groups. If the commensurability index $c(\Lambda, \Gamma)$ is finite, we say that the R-modules Λ and Γ are *commensurable* (in the strict sense as submodules of M). From now on assume that R is an integral domain with fraction field K and consider the pair (K^d, R^d) of R-modules for some integer $d > 0$. For an R-submodule Λ of K^d we abbreviate $c(\Lambda, R^d)$ by $c(\Lambda)$. The next proposition gives a necessary and sufficient condition on the ring R to describe the set $\mathcal{L}(K^d)$ in an alternative way using the commensurability index. Recall that $\mathcal{L}(K^d)$ is defined as the set of all R-submodules of K^d which are finitely generated and contain a basis of K^d.

Theorem 4.2.10. *Let R be an integral domain with fraction field K, let $d > 0$ be an integer and let $\Lambda \subseteq K^d$ be a non-zero R-submodule. If the two conditions*

(1) R is infinite if $d > 1$;

(2) for every non-zero ideal $I \subseteq R$ we have $|R : I| < \infty$;

both hold, then we have the equivalence

$$\Lambda \in \mathcal{L}(K^d) \Leftrightarrow c(\Lambda, R^d) < \infty.$$

Conversily, if the equivalence in (4.3) *holds, then the ring R satisfies the conditions* (1) *and* (2)*.*

Examples of rings satisfying conditions (1) and (2) are, for example, rings of integers of global fields and of non-Archimedean local fields.

Proof. Suppose first that the equivalence in (4.3) holds. If $d > 1$, then the ring R must be infinite, because otherwise $\Lambda = R^{d-1} \oplus \{0\}$ is a counterexample to the implication "$\Leftarrow$" (Λ does not contain a basis of K^d). This shows that condition (1) is necessary. Let $I \subseteq R$ be a non-zero finitely generated ideal of R, then clearly $I^d \in \mathcal{L}(K^d)$ and hence

$$|R : I|^d = |R^d : I^d| = c(I^d, R^d) < \infty,$$

that is $|R : I| < \infty$. Next let $J \subseteq R$ be an arbitrary non-zero ideal of R and $I \subseteq J$ a finitely generated ideal of R, then $|R : J| \leq |R : I| < \infty$. This shows that condition (2) is necessary.

Next, suppose that conditions (1) and (2) both hold. We first prove the implication "$\Rightarrow$" in (4.3). Assume that Λ is generated by $\ell > 0$ elements. Because K is the fraction field of R, we can find a non-zero element $a \in R$ such that $a\Lambda \subseteq R^d$. We then have

$$|\Lambda : \Lambda \cap R^d| \leq |\Lambda : a\Lambda| \leq |R : Ra|^\ell < \infty,$$

using condition (2) in the last step. Next, suppose that $\{b_1, \ldots, b_d\}$ is a basis of K^d contained in Λ and write $B \in \mathrm{GL}_d(K)$ for the matrix with columns $b_1, \ldots, b_d$. Multiplying

with a suitable non-zero element from R if necessary, we may assume without loss of generality that $b_i \in R^d$ for $i = 1, \ldots, d$. If $e_i \in K^d$ is the standard basis vector with entry 1 in the i-th position and entries zeroes otherwise, then for every i the equation $Bx = \det(B)e_i$ has a solution $x = x_i \in R^d$, because $b_i \in R^d$ implies $\det(B)B^{-1} = \mathrm{adj}(B) \in \mathrm{Mat}_d(R)$, here $\mathrm{adj}(B)$ stands for the adjugate of B, and hence $x_i = \mathrm{adj}(B)e_i \in R^d$. This shows that $\det(B)R^d \subseteq \Lambda$ and therefore we find similarly that

$$|R^d : \Lambda \cap R^d| \leq |R^d : \det(B)R^d| = |R : R\det(B)|^d < \infty$$

using condition (2) in the last step. It follows that $c(\Lambda, R^d) < \infty$.

Next we show that the implication "$\Leftarrow$" in (4.3) holds under the assumption that conditions (1) and (2) both hold. Assume that Λ satisfies $c(\Lambda, R^d) < \infty$ and suppose that $\Lambda \cap R^d$ does not contain a basis of K^d. If $d = 1$, then any non-zero element of K is a basis of K, hence we must have $\Lambda \cap R = \{0\}$. This is impossible, because Λ is assumed to be non-zero and hence, by multiplying with a suitable scalar, Λ must contain a non-zero element from Λ. For $d > 1$ we also derive a contradiction. We have $K(\Lambda \cap R^d) \neq K^d$ and hence there exists a non-zero vector $x \in R^d$ such that $Kx \cap (\Lambda \cap R^d) = \{0\}$. For $a, b \in R$ this gives

$$ax = bx \mod (\Lambda \cap R^d) \Leftrightarrow a = b$$

and since R is infinite, this implies that $R^d/(\Lambda \cap R^d)$ is infinite. This contradicts $|R^d : \Lambda \cap R^d| \leq c(\Lambda, R^d) < \infty$. Hence $\Lambda \cap R^d$, and therefore also Λ, contains a basis of K^d. Under the assumption that Λ contains a basis of K^d, we find analogously to the first paragraph that $bR^d \subseteq \Lambda$ for some non-zero element $b \in R$ and hence using (2) again

$$|\Lambda \cap R^d : bR^d| \leq |R^d : bR^d| = |R : Rb|^d < \infty.$$

Together with the fact that bR^d is finitely generated as an R-module, we find that $\Lambda \cap R^d$ is also finitely generated as an R-module. □

Let $d > 0$ be an integer and suppose that K is a non-Archimedean local field with ring of integers $\mathcal{O}$ and residue field of cardinality q. The next lemma shows that the commensurability index $c(\Lambda, \Gamma)$ of two $\mathcal{O}$-lattices $\Lambda, \Gamma \in \mathcal{L}(K^d)$ is a power of q. For convenience we introduce the integer $\widetilde{c}(\Lambda, \Gamma)$ defined by

$$q^{\widetilde{c}(\Lambda,\Gamma)} = c(\Lambda, \Gamma)$$

and we use the abbreviation $\widetilde{c}(\Lambda) = \widetilde{c}(\Lambda, \mathcal{O}^d)$.

Lemma 4.2.11. *Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$. Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice and let $g \in F(\Lambda)$ be a frame of Λ with corresponding signature matrix $D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$ for integers $e_1, \ldots, e_d \in \mathbf{Z}$ and a uniformiser $\pi \in \mathcal{O}$ of the maximal ideal of $\mathcal{O}$. The commensurability index $\widetilde{c}(\Lambda)$ is given by*

$$\widetilde{c}(\Lambda) = |e_1| + \ldots + |e_d|.$$

Proof. The element g is a frame for $\mathcal{O}^d$ and Λ and hence also of the $\mathcal{O}$-lattice $\Lambda \cap \mathcal{O}^d$. The signature matrix of $\Lambda \cap \mathcal{O}^d$ with respect to the frame g is the matrix $\mathrm{diag}(\pi^{m_1}, \ldots, \pi^{m_d})$, where $m_i = \max\{0, e_i\}$, because $\pi^{e_i}\mathcal{O} \cap \mathcal{O} = \pi^{m_i}\mathcal{O}$. Any element $h \in \mathrm{GL}_d(K)$ is an automorphism of the vector space K^d, so for two $\mathcal{O}$-lattices $\Gamma, \Sigma \in \mathcal{L}(K^d)$ we have

$$|\Gamma : \Sigma| = |h\Gamma : h\Sigma|,$$

where $h\Gamma, h\Sigma$ are the images of respectively Γ, Σ under the linear map h. Applying this to the element $h = g^{-1}$ we get

$$|\mathcal{O}^d : \Lambda \cap \mathcal{O}^d| = |\mathcal{O}^d : \bigoplus_{i=1}^{d} \pi^{m_i}\mathcal{O}| = \prod_{i=1}^{d} |\mathcal{O} : \pi^{m_i}\mathcal{O}| = q^{m_1+\ldots+m_d}$$

and

$$|\Lambda : \Lambda \cap \mathcal{O}^d| = |\bigoplus_{i=1}^{d} \pi^{e_i}\mathcal{O}^d : \bigoplus_{i=1}^{d} \pi^{m_i}\mathcal{O}| = \prod_{i=1}^{d} |\pi^{e_i}\mathcal{O} : \pi^{m_i}\mathcal{O}| = q^{(m_1-e_1)+\ldots+(m_d-e_d)}.$$

Together with the identity $2m_i - e_i = |e_i|$ this shows

$$q^{\widetilde{c}(\Lambda)} = q^{m_1+\ldots+m_d} \cdot q^{(m_1-e_1)+\ldots+(m_d-e_d)} = q^{|e_1|+\ldots+|e_d|}.$$

□

Lemma 4.2.12. *Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$. For each integer $n \geq 0$ the set*

$$\{\Lambda \in \mathcal{L}(K^d) \mid \widetilde{c}(\Lambda) = n\}$$

is finite.

Proof. For a fixed value of n, there are only finitely many tuples $(e_1, \ldots, e_d) \in \mathbf{Z}^d$ satisfying $\sum_{i=1}^{d} |e_i| = n$, so by Lemma 4.2.9 and Lemma 4.2.11 the number of signature matrices of a given $\mathcal{O}$-lattice $\Lambda \in \mathcal{L}(K^d)$ with $\widetilde{c}(\Lambda) = n$ is finite. This reduces the problem to showing, for a fixed signature matrix D, that the set

$$\{\Lambda \in \mathcal{L}(K^d) \mid D \text{ is signature matrix of } \Lambda\} \tag{4.4}$$

is finite. Write $G = \mathrm{GL}_d(\mathcal{O})$ and consider two elements $g, h \in G$. We have $gD\mathcal{O}^d = hD\mathcal{O}^d$ if and only if $D^{-1}h^{-1}gD\mathcal{O}^d = \mathcal{O}^d$, i.e. $D^{-1}h^{-1}gD \in G$, which is equivalent to $h^{-1}g \in DGD^{-1} \cap G$. This shows that the left cosets of $DGD^{-1} \cap G$ in G are in an one-to-one correspondence with the elements of the set in (4.4), the coset $g(DGD^{-1} \cap G)$ corresponds to the $\mathcal{O}$-lattice $gD\mathcal{O}^d$.

Next we show that for some integer $N \geq 0$ the congruence subgroup G_N is contained in $DGD^{-1} \cap G$. We will need the proof of this also for a later reference. Write $D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$ for some integers $e_i \in \mathbf{Z}$ and let $N = \max_{i \neq j}\{e_i - e_j\}$. If $N = 0$, then $D = \pi^e I$ for some integer $e \in \mathbf{Z}$, so $DGD^{-1} \cap G = G$ clearly has finite index in G. If

$N > 0$, then one verifies that $D^{-1}G_N D \leq G$, here $G_N = \mathrm{GL}_d^N(\mathcal{O})$ is the N-th principal congruence subgroup of $\mathrm{GL}_d(\mathcal{O})$; for a definition see Chapter 2. Hence $G_N \leq DGD^{-1} \cap G$ and because G_N has finite index in G, so does $DGD^{-1} \cap G$. This shows that there are only finitely many cosets $g(DGD^{-1} \cap G)$ and hence the set in (4.4) is finite. □

The next lemma gives an explicit description of the group $DGD^{-1} \cap G$, which occured in the proof of Lemma 4.2.12. This description will be useful for Proposition 4.4.3.

Lemma 4.2.13. *Let $d, \ell \geq 1$ be integers, let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and let π be a uniformiser for the maximal ideal of $\mathcal{O}$. Consider d ordered integers $e_1 \leq \ldots \leq e_d$ and ℓ pairwise different integers $a_1, \ldots, a_\ell$ such that $\{e_1, \ldots, e_d\} = \{a_1, \ldots, a_\ell\}$ and $a_1 < \ldots < a_\ell$, we write $m_i = |\{j \mid e_j = a_i\}|$. For the signature matrix $D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$ define the group $H = DGD^{-1} \cap G$ where $G = \mathrm{GL}_d(\mathcal{O})$. Then H consists of all matrices of the form*

$$\begin{pmatrix} H_{11} & H_{12} & \ldots & H_{1\ell} \\ H_{21} & H_{22} & & H_{2\ell} \\ \vdots & & \ddots & \vdots \\ H_{\ell 1} & H_{\ell 2} & \ldots & H_{\ell\ell} \end{pmatrix}$$

with $H_{ii} \in \mathrm{GL}_{m_i}(\mathcal{O})$ for $1 \leq i \leq \ell$, $H_{ij} \in \pi^{a_i - a_j}\mathrm{Mat}_{m_i m_j}(\mathcal{O})$ for $1 \leq j < i \leq \ell$ and $H_{ij} \in \mathrm{Mat}_{m_i m_j}(\mathcal{O})$ for $1 \leq i < j \leq \ell$.

Proof. Use block matrices to write out the effect of conjugating G with D to get a description for DGD^{-1} in terms of block matrices. Intersecting DGD^{-1} with G then gives the desired description. □

4.2.3 Commensurability zeta function

In the next two definitions we define the commensurability function, the corresponding commensurability zeta function and the submodule zeta function.

Definition 4.2.14. *Let R be a ring (commutative with 1) and let M be an R-module. Two R-submodules Λ, Γ of M are said to be* commensurable *(in the strict sense as submodules of M) if their commensurability index, $c(\Lambda, \Gamma)$, is finite. Fixing an R-submodule $N \subseteq M$, the* commensurability function $c^{M,N} : \mathbf{N} \to \mathbf{N} \cup \{\infty\} : n \mapsto c_n^{M,N}$ *is defined by*

$$c_n^{M,N} = |\{\Lambda \subseteq M \mid \Lambda \text{ an } R\text{-submodule, } c(\Lambda, N) = n\}|.$$

The commensurability zeta function *for the pair (M, N) of R-modules is defined by the generating function*

$$\zeta_{M,N}^{\mathrm{comm}}(s) = \sum_{n \geq 1} c_n^{M,N} n^{-s}, \quad s \in \mathbf{C}.$$

Definition 4.2.15. *Let R be a ring (commutative with 1) and let M be an R-module. The* submodule zeta function $\zeta_N^{\text{sub}}(s)$*, corresponding to the R-module M, is the generating function*

$$\zeta_M^{\text{sub}}(s) = \sum_{\Lambda \subseteq M} |M : \Lambda|^{-s}, \quad s \in \mathbf{C},$$

where we sum over all R-submodules $\Lambda \subseteq M$.

Note that in the previous definition we have $|M : \Lambda| = c(\Lambda, M)$ because $\Lambda \subseteq M$. The ring of integers of a global field or a non-Archimedean local field satisfies the conditions of Proposition 4.1.3. Therefore, we can give a different but equivalent definition for the commensurability zeta function and the submodule zeta function.

Corollary 4.2.16. *Let K be a global field or a non-Archimedean local field with ring of integers $\mathcal{O}$. The* commensurability zeta function $\zeta_{K^d,\mathcal{O}^d}^{\text{comm}}(s)$ *for the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules is also given by the generating function*

$$\zeta_{K^d,\mathcal{O}^d}^{\text{comm}}(s) = \sum_{\Lambda \in \mathcal{L}(K^d)} c(\Lambda, \mathcal{O}^d)^{-s}, \quad s \in \mathbf{C}$$

and the submodule zeta function $\zeta_{\mathcal{O}^d}^{\text{sub}}(s)$ *of $\mathcal{O}^d$ is the generating function*

$$\zeta_{\mathcal{O}^d}^{\text{sub}}(s) = \sum_{\Lambda \in \mathcal{L}(\mathcal{O}^d)} |\mathcal{O}^d : \Lambda|^{-s}, \quad s \in \mathbf{C}.$$

In case K is a non-Archimedean local field with residue field of cardinality q, define the formal series

$$Z_{K^d,\mathcal{O}^d}^{\text{comm}}(t) = \sum_{\Lambda \in \mathcal{L}(K^d)} t^{\widetilde{c}(\Lambda,\mathcal{O}^d)} \quad \text{and} \quad Z_{\mathcal{O}^d}^{\text{sub}}(t) = \sum_{\Lambda \in \mathcal{L}(\mathcal{O}^d)} t^{\widetilde{c}(\Lambda,\mathcal{O}^d)}.$$

These two series are related to the commensurability and submodule zeta function by

$$\zeta_{K^d,\mathcal{O}^d}^{\text{comm}}(s) = Z_{K^d,\mathcal{O}^d}^{\text{comm}}(q^{-s}) \quad \text{and} \quad \zeta_{\mathcal{O}^d}^{\text{sub}}(s) = Z_{\mathcal{O}^d}^{\text{sub}}(q^{-s}).$$

The next proposition determines the submodule zeta function in case K is a non-Archimedean local field.

Proposition 4.2.17. [27, Lem. 7.2] *Let $d > 0$ be an integer, K a non-Archimedean local field with ring of integers $\mathcal{O}$ and a residue field of cardinality q. We then have*

$$Z_{\mathcal{O}^d}^{\text{sub}}(t) = \prod_{k=0}^{d-1} \frac{1}{1 - q^k t}.$$

Remark 4.2.18. In the setting of the above proposition, note that we can write the statement also in the following two ways

$$Z^{\mathrm{sub}}_{\mathcal{O}^d}(t) = \prod_{k=0}^{d-1} Z^{\mathrm{sub}}_{\mathcal{O}}(q^k t) \quad \text{and} \quad \zeta^{\mathrm{sub}}_{\mathcal{O}^d}(s) = \prod_{k=0}^{d-1} \zeta^{\mathrm{sub}}_{\mathcal{O}}(s-k)$$

with $Z^{\mathrm{sub}}_{\mathcal{O}}(t) = \frac{1}{1-t}$ and $\zeta^{\mathrm{sub}}_{\mathcal{O}}(s) = \frac{1}{1-q^{-s}}$.

The next example shows that for a specific pair $(K, \mathcal{O})$ the associated commensurability zeta function differs depending upon whether we consider $K, \mathcal{O}$ as abelian groups or as $\mathcal{O}$-modules.

Example 4.2.19. Let K be a number field with $d = [K : \mathbf{Q}] > 1$ and let $\mathcal{O}$ be the ring of integers of K. The commensurability zeta function for the pair $(K, \mathcal{O})$ of $\mathcal{O}$-modules is (see Theorem 4.1.5) given by

$$\frac{\zeta_K(s)^2}{\zeta_K(2s)}, \tag{4.5}$$

here $\zeta_K(s)$ is the Dedekind zeta function of the number field K. The underlying abelian groups of K and $\mathcal{O}$ are isomorphic to $\mathbf{Q}^d$ and $\mathbf{Z}^d$ respectively. The commensurability zeta function for the pair $(K, \mathcal{O})$ of abelian groups is (see Corollary 4.1.2) given by

$$\prod_{i=0}^{d-1} \frac{\zeta(s-i)^2}{\zeta(2s-i)} \tag{4.6}$$

with $\zeta(s)$ is the Riemann zeta function. The two zeta functions $\zeta(s)$ and $\zeta_K(s)$ have an Euler product decomposition; see also Chapter 2. The local factors at the prime p are

$$\frac{1}{1-T} \quad \text{and} \quad \prod_{\mathfrak{p}|p} \frac{1}{1-T^{f(\mathfrak{p})}}$$

respectively, we used here the abbreviation $T = p^{-s}$ and the product runs over all prime ideals $\mathfrak{p}$ lying above p with $f(\mathfrak{p})$ denoting the inertia degree of $\mathfrak{p}$. The local factors of (4.6) and (4.5) at the prime p are thus

$$\prod_{i=0}^{d-1} \frac{1-p^i T^2}{(1-p^i T)^2} \quad \text{and} \quad \prod_{\mathfrak{p}|p} \frac{1-T^{2f(\mathfrak{p})}}{(1-T^{f(\mathfrak{p})})^2} \tag{4.7}$$

respectively. The rational function in T on the left in (4.7) has a pole at $T = p^{-1}$ of order at least one and the rational function in T on the right in (4.7) doesn't have a pole at $T = p^{-1}$. So the two local factors in (4.7) are different and consequently the zeta functions in (4.5) and (4.6) are different as well.

4.3 Euler product

In this section we establish the Euler product for the commensurability zeta function for a global field K. In preparation for this we first need a lemma. Lemma 4.3.1 shows that $\mathcal{O}$-lattices in K^d, of a fixed commensurability index with $\mathcal{O}^d$, are a fixed multiple away from $\mathcal{O}^d$.

Lemma 4.3.1. *Let $d, n > 0$ be integers and let K be a global or a non-Archimedean local field with ring of integers $\mathcal{O}$. There exists a non-zero element $m \in \mathcal{O}$ (depending only on d, n), such that for all $\mathcal{O}$-lattices $\Lambda, \Gamma \in \mathcal{L}(K^d)$ with $c(\Lambda, \Gamma) \mid n$ we have*

$$m\Gamma \subseteq \Lambda \quad \text{and} \quad m\Lambda \subseteq \Gamma. \tag{4.8}$$

Moreover, if K is a global field, then this element $m \in \mathcal{O} \subseteq K$ also fulfills the equivalent of equation (4.8) for any completion of K with respect to a maximal ideal of $\mathcal{O}$.

Proof. By the finiteness of the commensurability index $c(\Lambda, \Gamma)$, the quotient $\Lambda/\Lambda \cap \Gamma$ is a finite $\mathcal{O}$-module. The structure theorem for finitely generated modules over a Dedekind domain, see Chapter 2, therefore applies and hence

$$\Lambda/\Lambda \cap \Gamma \cong \bigoplus_{i=1}^{k} \mathcal{O}/I_i \tag{4.9}$$

for some non-zero ideals $I_i \subseteq \mathcal{O}$. Write $I = I_1 \cdots I_k$ for the product of the ideals I_i. Then I is non-zero, satisfies $|\Lambda : \Lambda \cap \Gamma| = \prod_{i=1}^{k} |\mathcal{O} : I_i| = |\mathcal{O} : I|$ and is contained in the annihilator of the right hand-side of (4.9) so that in fact $I\Lambda \subseteq \Lambda \cap \Gamma \subseteq \Gamma$. Analogously there exists a non-zero ideal $J \subseteq \mathcal{O}$ satisfying $J\Gamma \subseteq \Lambda \cap \Gamma \subseteq \Lambda$ and $|\Gamma : \Lambda \cap \Gamma| = |\mathcal{O} : J|$. Combining both inclusions, we find that the ideal $P = IJ$ satisfies $c(\Lambda, \Gamma) = |\mathcal{O} : P|$ and

$$P\Lambda \subseteq \Gamma \quad \text{and} \quad P\Gamma \subseteq \Lambda. \tag{4.10}$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ with $P \subseteq \mathfrak{p}^e$ for some integer $e \geq 1$, then

$$|\mathcal{O} : \mathfrak{p}|^e = |\mathcal{O} : \mathfrak{p}^e| \leq |\mathcal{O} : P| = c(\Lambda, \Gamma) \leq n.$$

This shows that both $|\mathcal{O} : \mathfrak{p}|$ and e are bounded from above by n. Write S for the set of all maximal ideals of $\mathcal{O}$. Because K is a global field or a non-Archimedean local field, the set $\{\mathfrak{p} \in S \mid |\mathcal{O} : \mathfrak{p}| \leq n\}$ is finite. Therefore the ideal

$$Q = \prod_{\mathfrak{p} \in S,\, |\mathcal{O}:\mathfrak{p}| \leq n} \mathfrak{p}^n$$

is a finite product of ideals satisfying $Q \subseteq P$. Let $m \in Q$ be a non-zero element, then $(m) \subseteq Q \subseteq P$ together with (4.10) implies $m\Gamma \subseteq \Lambda$ and $m\Lambda \subseteq \Gamma$.

Let K be a global field and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$. Write $K_\mathfrak{p}$ for the completion of K with respect to $\mathfrak{p}$ and write $\mathcal{O}_\mathfrak{p}$ for the ring of integers of $K_\mathfrak{p}$ and q for the cardinality of $\mathcal{O}/\mathfrak{p}$. Write Q_0, Q_1 for the ideal Q defined above in the case of K and $K_\mathfrak{p}$ respectively. If $|\mathcal{O} : \mathfrak{p}| \leq n$, then $\mathfrak{p}^n \mid Q$ so that $m \in Q \subseteq \mathfrak{p}^n \subseteq (\mathfrak{p}\mathcal{O}_\mathfrak{p})^n = Q_1$. If $|\mathcal{O} : \mathfrak{p}| > n$, then the only pairs (Λ, Γ) of $\mathcal{O}_\mathfrak{p}$-lattices satisfying $c(\Lambda, \Gamma) \mid n$ are those where $\Lambda = \Gamma$, using that $c(\Lambda, \Gamma)$ is a power of q. In this case any such non-zero $m \in \mathcal{O}$ works. □

Remark 4.3.2. The above proof contains a very generous way of producing Q. When K is a number field we can actually take $m = n$ in Lemma 4.3.1. Because the abelian group $\Lambda/\Lambda \cap \Gamma$ has exponent dividing $|\Lambda : \Lambda \cap \Gamma| \mid c(\Lambda, \Gamma) \mid n$, from which it follows that $n\Lambda \subseteq \Lambda \cap \Gamma \subseteq \Gamma$ and analogously $n\Gamma \subseteq \Lambda$.

The next proposition establishes an Euler product for the commensurability zeta function $\zeta^{\text{comm}}_{K^d,\mathcal{O}^d}(s)$ in the case that K is a global field and also for the submodule zeta function $\zeta^{\text{sub}}_{\mathcal{O}^d}(s)$. This Euler product is analogous to an Euler product we encountered in 4.1, for a different type of commensurability zeta function.

Proposition 4.3.3. *Let $d > 0$ be an integer and let K be a global field with ring of integers $\mathcal{O}$. We write S for the set of all maximal ideals of $\mathcal{O}$. The commensurability zeta function $\zeta^{\text{comm}}_{K^d,\mathcal{O}^d}(s)$ for the pair $(K^d, \mathcal{O}^d)$ has the formal Euler product*

$$\zeta^{\text{comm}}_{K^d,\mathcal{O}^d}(s) = \prod_{\mathfrak{p}\in S} \zeta^{\text{comm}}_{K^d_\mathfrak{p},\mathcal{O}^d_\mathfrak{p}}(s) \tag{4.11}$$

and the submodule zeta function $\zeta^{\text{sub}}_{\mathcal{O}^d}(s)$ has the formal Euler product

$$\zeta^{\text{sub}}_{\mathcal{O}^d}(s) = \prod_{\mathfrak{p}\in S} \zeta^{\text{sub}}_{\mathcal{O}^d_\mathfrak{p}}(s). \tag{4.12}$$

Proof. We will only prove the Euler product for the commensurability zeta function. The proof for the Euler product of the submodule zeta function $\zeta^{\text{sub}}_{\mathcal{O}^d}(s)$ can be proven in an analogous way.
Fix an integer $n > 0$ and write S for the set of all maximal ideals of $\mathcal{O}$. For $\mathfrak{p} \in S$ write $K_\mathfrak{p}$ for the completion of K with respect to $\mathfrak{p}$ with ring of integers $\mathcal{O}_\mathfrak{p}$. The coefficient of n^{-s} on the left hand-side of (4.11) equals the cardinality of the set

$$\{\Gamma \in \mathcal{L}(K^d) \mid c(\Gamma) = n\} \tag{4.13}$$

and the coefficient of n^{-s} in the right hand-side of (4.11) equals the cardinality of the set

$$\{(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S} \mid \Gamma_\mathfrak{p} \in \mathcal{L}(K^d_\mathfrak{p}), \prod_{\mathfrak{p}\in S} c(\Gamma_\mathfrak{p}, \mathcal{O}^d_\mathfrak{p}) = n\}. \tag{4.14}$$

For a maximal ideal $\mathfrak{p} \in S$ we have $c(\Gamma_\mathfrak{p}, \mathcal{O}^d_\mathfrak{p}) = 1$ if and only if $\Gamma_\mathfrak{p} = \mathcal{O}^d_\mathfrak{p}$, so an element $(\Gamma_\mathfrak{p})_{\mathfrak{p}\in S}$ of the set defined in (4.14) has $\Gamma_\mathfrak{p} = \mathcal{O}^d_\mathfrak{p}$ for all but finitely many $\mathfrak{p} \in S$. Using

the Chinese remainder theorem, we show below that there is a one-to-one correspondence between the sets in (4.13) and (4.14). The direction "⇒" of this correspondence is given by

$$\Lambda \mapsto (\mathcal{O}_\mathfrak{p}\Lambda)_{\mathfrak{p}\in S}.$$

This implies that both sets have the same cardinality and consequently the formal Euler product holds.

Define the $\mathcal{O}$-module $M = \frac{1}{m}\mathcal{O}^d$, here $m \in \mathcal{O}$ is a non-zero element which, by Lemma 4.3.1, can be chosen such that the inclusions

$$m^2M = m\mathcal{O}^d \subseteq \Lambda \subseteq \tfrac{1}{m}\mathcal{O}^d = M \tag{4.15}$$

hold for all $\mathcal{O}$-lattices $\Lambda \in \mathcal{L}(K^d)$ satisfying $c(\Lambda, \mathcal{O}^d) \mid n$. In the Dedekind domain $\mathcal{O}$ we can factor the ideal $m\mathcal{O}$ as

$$m\mathcal{O} = \prod_{\mathfrak{p}\in T} \mathfrak{p}^{e_\mathfrak{p}}$$

for some finite subset $T \subseteq S$ with multiplicities $e_\mathfrak{p} > 0$. For every maximal ideal $\mathfrak{p} \in S$ define the $\mathcal{O}$-module

$$M_\mathfrak{p} = \mathcal{O}_\mathfrak{p}M = \tfrac{1}{m}\mathcal{O}_\mathfrak{p}^d \subseteq K_\mathfrak{p}^d.$$

Note that by extension of scalars we can consider $M_\mathfrak{p}$ also as an $\mathcal{O}_\mathfrak{p}$-module and hence the same holds for any quotient module of $M_\mathfrak{p}$. By the second part of Lemma 4.3.1 the element m can also be used for all completions $K_\mathfrak{p}$ of K. This means that for any $\mathfrak{p} \in S$ and any $\mathcal{O}_\mathfrak{p}$-lattice $\Lambda_\mathfrak{p} \in \mathcal{L}(K_\mathfrak{p}^d)$ satisfying $c(\Lambda_\mathfrak{p}, \mathcal{O}_\mathfrak{p}^d) \mid n$, we have the inclusions

$$m^2M_\mathfrak{p} = m\mathcal{O}_\mathfrak{p}^d \subseteq \Lambda_\mathfrak{p} \subseteq \tfrac{1}{m}\mathcal{O}_\mathfrak{p}^d = M_\mathfrak{p}.$$

Note that if $\mathfrak{p} \in S\backslash T$, then $m \in \mathcal{O}_\mathfrak{p}^*$ so that $\Lambda_\mathfrak{p} = \mathcal{O}_\mathfrak{p}^d$ and therefore $c(\Lambda_\mathfrak{p}, \mathcal{O}_\mathfrak{p}^d) = 1$. This shows that the set in (4.14) is in bijection with the set

$$\{(\Lambda_\mathfrak{p})_{\mathfrak{p}\in T} \mid \Lambda_\mathfrak{p} \in \mathcal{L}(K_\mathfrak{p}^d), \prod_{\mathfrak{p}\in T} c(\Lambda_\mathfrak{p}, \mathcal{O}_\mathfrak{p}^d) = n\}. \tag{4.16}$$

We have $m\mathcal{O}_\mathfrak{p} = \mathfrak{p}^{e_\mathfrak{p}}\mathcal{O}_\mathfrak{p}$ for $\mathfrak{p} \in T$ and $m\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$ for $\mathfrak{p} \in S\backslash T$, hence $m^2M_\mathfrak{p} = \mathfrak{p}^{2e_\mathfrak{p}}M_\mathfrak{p}$ for $\mathfrak{p} \in T$. For $\mathfrak{p} \in T$ we have that $\mathcal{O} \subseteq \mathcal{O}_\mathfrak{p}$ is dense, so extension and restriction of scalars induce a bijection between the $\mathcal{O}$-submodules and the $\mathcal{O}_\mathfrak{p}$-submodules of $M_\mathfrak{p}/\mathfrak{p}^{2e_\mathfrak{p}}M_\mathfrak{p}$. Moreover, for $\mathfrak{p} \in T$ the inclusion $\mathcal{O}^d \subseteq \mathcal{O}_\mathfrak{p}^d$ induces an isomorphism $M/\mathfrak{p}^{2e_\mathfrak{p}}M \cong M_\mathfrak{p}/\mathfrak{p}^{2e_\mathfrak{p}}M_\mathfrak{p}$ of $\mathcal{O}$-modules.

Any $\mathcal{O}$-submodule of M/m^2M is of the form Λ/m^2M for some $\mathcal{O}$-submodule Λ of K^d satisfying the inclusions in (4.15). In fact, we have in this case $\Lambda \in \mathcal{L}(K^d)$, because $m\mathcal{O}^d \subseteq \Lambda$ shows that Λ contains a basis of K^d and $|M : m^2M| = |\mathcal{O}^d : m^2\mathcal{O}^d| < \infty$ shows that Λ is finitely generated. Using that $c(\Lambda, \mathcal{O}^d) = c(\Lambda/m^2M, \mathcal{O}^d/m^2M)$, we see that $\Lambda \mapsto \Lambda/m^2M$ induces a bijection between the set in (4.13) and

$$\{\mathcal{O}\text{-submodule } A \subseteq M/m^2M \mid c(A, \mathcal{O}^d/m^2M) = n\}. \tag{4.17}$$

Similarly, the map $(\Lambda_\mathfrak{p})_{\mathfrak{p}\in T} \mapsto (\Lambda_\mathfrak{p}/m^2M_\mathfrak{p})_{\mathfrak{p}\in T}$ induces a bijection between the set in (4.16) and

$$\{\mathcal{O}\text{-submodule } (A_\mathfrak{p})_{\mathfrak{p}\in T} \subseteq (M_\mathfrak{p}/m^2M_\mathfrak{p})_{\mathfrak{p}\in T} \mid \prod_{\mathfrak{p}\in T} c(A_\mathfrak{p}, \mathcal{O}_\mathfrak{p}^d/m^2M_\mathfrak{p}) = n\}. \tag{4.18}$$

So it remains to show that there is a bijection between the sets (4.17) and (4.18).

Because different maximal ideals are coprime, the Chinese remainder theorem for modules gives us the isomorphism of $\mathcal{O}$-modules

$$M/m^2M \cong \bigoplus_{\mathfrak{p}\in T} M/\mathfrak{p}^{2e_\mathfrak{p}}M \cong \bigoplus_{\mathfrak{p}\in T} M_\mathfrak{p}/\mathfrak{p}^{2e_\mathfrak{p}}M_\mathfrak{p} = \bigoplus_{\mathfrak{p}\in T} M_\mathfrak{p}/m^2M_\mathfrak{p}, \tag{4.19}$$

under which Λ/m^2M, for an $\mathcal{O}$-submodule Λ of M with $m^2M \subseteq \Lambda$, is mapped according to

$$\Lambda/m^2M \mapsto \bigoplus_{\mathfrak{p}\in T}(\Lambda + \mathfrak{p}^{2e_\mathfrak{p}}M)/\mathfrak{p}^{2e_\mathfrak{p}}M \mapsto \bigoplus_{\mathfrak{p}\in T} \mathcal{O}_\mathfrak{p}\Lambda/\mathfrak{p}^{2e_\mathfrak{p}}M_\mathfrak{p} = \bigoplus_{\mathfrak{p}\in T} \mathcal{O}_\mathfrak{p}\Lambda/m^2M_\mathfrak{p}.$$

Here we used for the last map that $m^2M \subseteq \Lambda$ implies $\mathfrak{p}^{2e_\mathfrak{p}}M_\mathfrak{p} \subseteq \mathcal{O}_\mathfrak{p}\Lambda$. The isomorphism in (4.19) shows, for an $\mathcal{O}$-submodule $\bigoplus_{\mathfrak{p}\in T} A_\mathfrak{p}$ of the right hand-side of (4.19), that there exists a corresponding $\mathcal{O}$-submodule A of M/m^2M satisfying $A_\mathfrak{p} = \mathcal{O}_\mathfrak{p}A$ for all $\mathfrak{p} \in T$. Consider an $\mathcal{O}$-submodule A of M/m^2M and write $A_\mathfrak{p} = \mathcal{O}_\mathfrak{p}A$ for $\mathfrak{p} \in T$, then

$$c(A, \mathcal{O}^d/m^2M) = c(\bigoplus_{\mathfrak{p}\in T} A_\mathfrak{p}, \bigoplus_{\mathfrak{p}\in T} \mathcal{O}_\mathfrak{p}^d/m^2M_\mathfrak{p}) = \prod_{\mathfrak{p}\in T} c(A_\mathfrak{p}, \mathcal{O}_\mathfrak{p}^d/m^2M_\mathfrak{p}). \tag{4.20}$$

This gives the desired bijection between (4.17) and (4.18). □

4.4 Local commensurability zeta function

Let $d > 0$ be an integer. Throughout this section we write K for a non-Archimedean local field with ring of integers $\mathcal{O}$ and we let π be a uniformiser of the maximal ideal of $\mathcal{O}$. Moreover, L is a global field with ring of integers $\mathcal{O}_L$. The Euler product, established in the previous section, reduces the problem of computing the commensurability zeta function of the pair $(L^d, \mathcal{O}_L^d)$ of $\mathcal{O}_L$-modules to computing the commensurability zeta function of the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules. In this section we show that the commensurability zeta function of the pair $(K^d, \mathcal{O}^d)$ of $\mathcal{O}$-modules can be expressed in terms of the submodule zeta function for $\mathcal{O}^d$ as an $\mathcal{O}$-module.

Lemma 4.4.1. *Let $d > 0$ be an integer and let $\Lambda, \Gamma \in \mathcal{L}(\mathcal{O}^d)$ be two $\mathcal{O}$-lattices and write $\Sigma = \Lambda + \Gamma$ for their sum, which is also an $\mathcal{O}$-lattice in $\mathcal{L}(\mathcal{O}^d)$. We have the following relation between the commensurability indices*

$$\widetilde{c}(\Lambda) + \widetilde{c}(\Gamma) = 2\widetilde{c}(\Sigma) + \widetilde{c}(\Lambda, \Gamma).$$

Proof. From the isomorphism theorem for modules we get $\Sigma/\Lambda \cong \Gamma/(\Lambda \cap \Gamma)$ and similarly $\Sigma/\Gamma \cong \Lambda/(\Lambda \cap \Gamma)$. One then computes

$$\begin{aligned} |\mathcal{O}^d : \Lambda||\mathcal{O}^d : \Gamma| &= |\mathcal{O}^d : \Sigma||\Sigma : \Lambda||\mathcal{O}^d : \Sigma||\Sigma : \Gamma| = |\mathcal{O}^d : \Sigma|^2|\Sigma : \Lambda||\Sigma : \Gamma| \\ &= |\mathcal{O}^d : \Sigma|^2|\Lambda : \Lambda \cap \Gamma||\Gamma : \Lambda \cap \Gamma| = |\mathcal{O}^d : \Sigma|^2 c(\Lambda, \Gamma) \end{aligned} \tag{4.21}$$

and so we find

$$\widetilde{c}(\Lambda) + \widetilde{c}(\Gamma) = 2\widetilde{c}(\Sigma) + \widetilde{c}(\Lambda, \Gamma).$$

□

The next proposition establishes a bijection between certain $\mathcal{O}$-lattices in K^d and pairs of $\mathcal{O}$-lattices in $\mathcal{O}^d$. Recall from Section 4.2.1 that an $\mathcal{O}$-lattice is a finitely generated $\mathcal{O}$-submodule of K^d containing a basis of K^d. If $\Lambda \in \mathcal{L}(K^d)$ is such an $\mathcal{O}$-lattice, then we write $F(\Lambda)$ for the set of all frames of Λ. A frame $g \in F(\Lambda)$ is an element of $\mathrm{GL}_d(\mathcal{O})$ such that we can write $\Lambda = gD\mathcal{O}^d$ for some signature matrix D.

Proposition 4.4.2. *Let $d > 0$ be an integer. For an element $g \in \mathrm{GL}_d(\mathcal{O})$ consider the sets*

$$A_g = \{\Lambda \in \mathcal{L}(K^d) \mid g \in F(\Lambda)\}$$

of all $\mathcal{O}$-lattices in $\mathcal{L}(K^d)$ having g as a frame and

$$B_g = \{(\Gamma, \Sigma) \in \mathcal{L}(\mathcal{O}^d) \times \mathcal{L}(\mathcal{O}^d) \mid g \in F(\Gamma) \cap F(\Sigma), \Gamma + \Sigma = \mathcal{O}^d\}.$$

There exists a bijection $\varphi_g : A_g \to B_g$ preserving the commensurability index: if $\varphi_g(\Lambda) = (\Gamma, \Sigma)$ then

$$\widetilde{c}(\Lambda) = \widetilde{c}(\Gamma) + \widetilde{c}(\Sigma) = \widetilde{c}(\Gamma, \Sigma).$$

Proof. Let π be a uniformiser of the maximal ideal of $\mathcal{O}$. For the $\mathcal{O}$-lattice $\Lambda \in A_g$ let $D = \mathrm{diag}(\pi^{e_1}, \ldots, \pi^{e_d})$ with $e_i \in \mathbf{Z}$ be the corresponding signature matrix of $g \in F(\Lambda)$. Define the two signature matrices $D_\pm$ by

$$D_\pm = \mathrm{diag}(\pi^{\max\{0, \pm e_1\}}, \ldots, \pi^{\max\{0, \pm e_d\}})$$

and write $\Lambda_\pm = gD_\pm\mathcal{O}^d \in \mathcal{L}(\mathcal{O}^d)$. These $\mathcal{O}$-lattices Λ_-, Λ_+ satisfy $\Lambda_- + \Lambda_+ = \mathcal{O}^d$ since $\pi^{\max\{0,-e_i\}}\mathcal{O} + \pi^{\max\{0,e_i\}}\mathcal{O} = \mathcal{O}$. Define the map

$$\varphi_g : A_g \to B_g, \varphi_g(\Lambda) = (\Lambda_-, \Lambda_+),$$

then φ_g is by construction injective (D can be recovered from $D_\pm$ through $D = D_-^{-1}D_+$). That φ_g preserves the commensurability index follows from Lemma 4.4.1, applied to Λ_-, Λ_+ and $\Lambda_- + \Lambda_+ = \mathcal{O}^d$, and

$$\widetilde{c}(\Lambda) = \sum_{i=1}^{d} |e_i| = \sum_{i=1}^{d} \max\{0, -e_i\} + \sum_{i=1}^{d} \max\{0, e_i\} = \widetilde{c}(\Lambda_-) + \widetilde{c}(\Lambda_+)$$

by Lemma 4.2.11.

For a pair $(\Gamma, \Sigma) \in B_g$ there exist by definition unique signature matrices E, F such that $\Gamma = gE\mathcal{O}^d$ and $\Sigma = gF\mathcal{O}^d$. The condition $\Gamma + \Sigma = \mathcal{O}^d$ is equivalent to $E\mathcal{O}^d + F\mathcal{O}^d = \mathcal{O}^d$. Write $E = \mathrm{diag}(\pi^{a_1}, \ldots, \pi^{a_d})$ and $F = \mathrm{diag}(\pi^{b_1}, \ldots, \pi^{b_d})$ for some integers $a_i, b_i \in \mathbf{Z}_{\geq 0}$, then $\min\{a_i, b_i\} = 0$ for every i. Define the $\mathcal{O}$-lattice $\Lambda = gE^{-1}F\mathcal{O}^d$. One verifies that $E = (E^{-1}F)_-$, $F = (E^{-1}F)_+$ and hence $\varphi(\Lambda) = (\Gamma, \Sigma)$. It follows that φ_g is surjective. $\square$

Recall that the profinite group $\mathrm{GL}_d(\mathcal{O})$ can be equipped with a Haar measure μ, which we conveniently normalise by $\mu(\mathrm{GL}_d(\mathcal{O})) = 1$. For a subset $\Omega \subseteq \mathrm{GL}_d(\mathcal{O})$ we write $\mathbf{1}_\Omega$ for the characteristic function of Ω. When Ω is a μ-measurable set, we have the identity

$$\int_{\mathrm{GL}_d(\mathcal{O})} \mathbf{1}_\Omega(x)\, d\mu = \mu(\Omega).$$

The next proposition says that two sets of frames in $\mathrm{GL}_d(\mathcal{O})$ have the same Haar measure. This is a key part in the proof of Theorem 4.1.5.

Proposition 4.4.3. *Let $\Lambda \in \mathcal{L}(K^d)$ be an $\mathcal{O}$-lattice, let $g \in F(\Lambda)$ be a frame for Λ and write φ_g for the bijection from Proposition 4.4.2. If $\varphi_g(\Lambda) = (\Gamma, \Sigma)$ for two $\mathcal{O}$-lattices $\Lambda, \Gamma \in \mathcal{L}(\mathcal{O}^d)$, then the sets $F(\Lambda)$ and $F(\Gamma, \Sigma)$ are both μ-measurable and moreover*

$$\mu(F(\Lambda)) = \mu(F(\Gamma, \Sigma)) > 0.$$

We postpone the proof of Proposition 4.4.3 for now. First we prove Theorem 4.1.5, under the assumption that Proposition 4.4.3 holds.

Proof of Theorem 4.1.5. Proposition 4.1.4 shows that, in order to calculate the commensurability zeta function in the global case, we may reduce to the local setting. By Proposition 4.2.17 we have $Z^{\mathrm{sub}}_{\mathcal{O}^d}(t) \in \mathbf{Z}[\![t]\!]$. Using Lemma 4.4.1 for the third equality below, we find

$$\begin{aligned} Z^{\mathrm{sub}}_{\mathcal{O}^d}(t)^2 &= \sum_{\Lambda,\Gamma \in \mathcal{L}(\mathcal{O}^d)} t^{\widetilde{c}(\Lambda)+\widetilde{c}(\Gamma)} = \sum_{\Sigma \in \mathcal{L}(\mathcal{O}^d)} \sum_{\substack{\Lambda,\Gamma \in \mathcal{L}(\mathcal{O}^d),\\ \Lambda+\Gamma=\Sigma}} t^{\widetilde{c}(\Lambda)+\widetilde{c}(\Gamma)} \\ &= \sum_{\Sigma \in \mathcal{L}(\mathcal{O}^d)} \sum_{\substack{\Lambda,\Gamma \in \mathcal{L}(\mathcal{O}^d),\\ \Lambda+\Gamma=\Sigma}} t^{2\widetilde{c}(\Sigma)+\widetilde{c}(\Lambda,\Gamma)} = \sum_{\Sigma \in \mathcal{L}(\mathcal{O}^d)} t^{2\widetilde{c}(\Sigma)} \sum_{\substack{\Lambda,\Gamma \in \mathcal{L}(\mathcal{O}^d),\\ \Lambda+\Gamma=\Sigma}} t^{\widetilde{c}(\Lambda,\Gamma)}. \end{aligned}$$

Note that for $\mathcal{O}$-lattices Λ, Γ, Σ, the condition $\Lambda + \Gamma = \Sigma$ implies $\Lambda, \Gamma \subseteq \Sigma$. Let $\Sigma \in \mathcal{L}(\mathcal{O}^d)$ be an $\mathcal{O}$-lattice, then there exists an $\mathcal{O}$-module isomorphism $\psi : \Sigma \to \mathcal{O}^d$ and clearly any such isomorphism preserves the commensurability index associated to sublattice pairs in

Σ, i.e. $c(\Lambda,\Gamma) = c(\psi(\Lambda),\psi(\Gamma))$ for all $\mathcal{O}$-submodules $\Lambda,\Gamma \subseteq \Sigma$. Consequently, for any $\mathcal{O}$-lattice $\Sigma \in \mathcal{L}(\mathcal{O}^d)$ we have the equality

$$\sum_{\substack{\Lambda,\Gamma\in\mathcal{L}(\mathcal{O}^d),\\ \Lambda+\Gamma=\Sigma}} t^{\widetilde{c}(\Lambda,\Gamma)} = \sum_{\substack{\Lambda,\Gamma\in\mathcal{L}(\mathcal{O}^d),\\ \Lambda+\Gamma=\mathcal{O}^d}} t^{\widetilde{c}(\Lambda,\Gamma)} \tag{4.22}$$

and we abbreviate the latter series in $\mathbf{Z}[\![t]\!]$ by

$$Z^{\mathrm{rel}}_{\mathcal{O}^d}(t) = \sum_{\substack{\Lambda,\Gamma\in\mathcal{L}(\mathcal{O}^d),\\ \Lambda+\Gamma=\mathcal{O}^d}} t^{\widetilde{c}(\Lambda,\Gamma)}.$$

We call the series $Z^{\mathrm{rel}}_{\mathcal{O}^d}(t)$ the *relative zeta function*, because the condition $\Lambda+\Gamma=\mathcal{O}^d$ is reminiscent of two ideals being relatively prime. This shows that the series $Z^{\mathrm{sub}}_{\mathcal{O}^d}(t)^2$ can be rewritten as

$$Z^{\mathrm{sub}}_{\mathcal{O}^d}(t)^2 = Z^{\mathrm{rel}}_{\mathcal{O}^d}(t) \sum_{\Sigma\in\mathcal{L}(\mathcal{O}^d)} t^{2\widetilde{c}(\Sigma)} = Z^{\mathrm{rel}}_{\mathcal{O}^d}(t) Z^{\mathrm{sub}}_{\mathcal{O}^d}(2t).$$

In order to prove the local formula for the commensurability zeta function, it remains to show that $Z^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(t) = Z^{\mathrm{rel}}_{\mathcal{O}^d}(t)$.

Let $n \geq 0$ be an integer, define the sets

$$C_n = \{\Lambda \in \mathcal{L}(K^d) \mid \widetilde{c}(\Lambda) = n\}$$

and

$$D_n = \{(\Gamma,\Sigma) \in \mathcal{L}(\mathcal{O}^d)\times\mathcal{L}(\mathcal{O}^d) \mid \Gamma+\Sigma = \mathcal{O}^d \text{ and } \widetilde{c}(\Gamma,\Sigma) = n\}.$$

Then $|C_n|, |D_n|$ are the coefficients of t^n in the series $Z^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(t), Z^{\mathrm{rel}}_{\mathcal{O}^d}(t)$ respectively and, in particular, they are finite.

Let $g \in \mathrm{GL}_d(\mathcal{O})$ be any element and let $n \geq 0$ be some integer. The bijection $\varphi_g : A_g \to B_g$ in Lemma 4.4.2 preserves the commensurability index, so we can restrict φ_g to $\mathcal{O}$-lattices $\Lambda \in \mathcal{L}(\mathcal{O}^d)$ with $\widetilde{c}(\Lambda) = n$. This gives a bijection between $A_g \cap C_n$ and $B_g \cap D_n$; by Lemma 4.2.12 these sets are finite since C_n is a finite set. If $\varphi_g(\Lambda) = (\Gamma,\Sigma)$, then $\mu(F(\Lambda)) = \mu(F(\Gamma,\Sigma)) > 0$ by Proposition 4.4.3. Together this results in the identity

$$\sum_{\Lambda\in C_n} \frac{\mathbf{1}_{F(\Lambda)}(g)}{\mu(F(\Lambda))} = \sum_{\Lambda\in C_n\cap A_g} \frac{1}{\mu(F(\Lambda))} = \sum_{(\Gamma,\Sigma)\in D_n\cap B_g} \frac{1}{\mu(F(\Gamma,\Sigma))} = \sum_{(\Gamma,\Sigma)\in D_n} \frac{\mathbf{1}_{F(\Gamma,\Sigma)}(g)}{\mu(F(\Gamma,\Sigma))}$$

for any $g \in \mathrm{GL}_d(\mathcal{O})$. Taking the integral of the identity above (as a function of g) over the

group $\mathrm{GL}_d(\mathcal{O})$ gives

$$\begin{aligned}|C_n| &= \sum_{\Lambda\in C_n}\int_{\mathrm{GL}_d(\mathcal{O})}\frac{\mathbf{1}_{F(\Lambda)}(g)}{\mu(F(\Lambda))}d\mu(g)\\ &= \int_{\mathrm{GL}_d(\mathcal{O})}\sum_{\Lambda\in C_n}\frac{\mathbf{1}_{F(\Lambda)}(g)}{\mu(F(\Lambda))}d\mu(g) = \int_{\mathrm{GL}_d(\mathcal{O})}\sum_{(\Gamma,\Sigma)\in D_n}\frac{\mathbf{1}_{F(\Gamma,\Sigma)}(g)}{\mu(F(\Gamma,\Sigma))}d\mu(g)\\ &= \sum_{(\Gamma,\Sigma)\in D_n}\int_{\mathrm{GL}_d(\mathcal{O})}\frac{\mathbf{1}_{F(\Gamma,\Sigma)}(g)}{\mu(F(\Gamma,\Sigma))}d\mu(g) = |D_n|.\end{aligned}$$

Note that interchanging the sum and the integral is allowed, because the sets C_n, D_n are finite. It follows that $Z^{\mathrm{comm}}_{K^d}(t) = Z^{\mathrm{rel}}_{\mathcal{O}^d}(t)$, so

$$Z^{\mathrm{sub}}_{\mathcal{O}^d}(t)^2 = Z^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(t)Z^{\mathrm{sub}}_{\mathcal{O}^d}(2t)$$

and hence we conclude that

$$\zeta^{\mathrm{sub}}_{\mathcal{O}^d}(s)^2 = \zeta^{\mathrm{comm}}_{K^d,\mathcal{O}^d}(s)\zeta^{\mathrm{sub}}_{\mathcal{O}^d}(2s).$$

□

Before reading the second part of the proof of Proposition 4.4.3, look at Example 4.4.4 for an illustration of the second part.

Proof of Proposition 4.4.3. Write $G = \mathrm{GL}_d(\mathcal{O})$ and $\varphi_g(\Lambda) = (\Lambda_-, \Lambda_+)$, where the $\mathcal{O}$-lattices $\Lambda, \Lambda_\pm$ have the signature matrices $D, D_\pm$ with respect to the frame g. Furthermore, denote by P the collection of all signature matrices corresponding to the $\mathcal{O}$-lattice Λ and by Q the collection of all pairs of signature matrices (with respect to the same frame) corresponding to the pair (Λ_-, Λ_+) of $\mathcal{O}$-lattices. Any element $E \in P$ is obtained through a permutation of the diagonal entries of D and any element $(E_-, E_+) \in Q$ arises as a permutation of the diagonal entries of the pair (D_-, D_+). From the proof of Proposition 4.4.2 it follows that there is a bijection between P and Q given by $E \leftrightarrow (E_-, E_+)$ with $E = E_-^{-1}E_+$. This shows that P and Q are finite sets of the same cardinality.

Define the groups $H = DGD^{-1} \cap G$, $H_\pm = D_\pm G D_\pm^{-1} \cap G$ and $T = H_- \cap H_+$. Let $h \in G$ be another frame for Λ with corresponding signature matrix E, so $\Lambda = hE\mathcal{O}^d$. By a similar argument as in the the proof of Lemma 4.2.12 (directly after (4.4)) this is equivalent to $h \in g(DGE^{-1} \cap G)$. Let $\sigma_E \in G$ be a permutation matrix such that $E = \sigma_E^{-1} D \sigma_E$, then

$$g(DGE^{-1} \cap G) = g(DGD^{-1} \cap G)\sigma_E = gH\sigma_E.$$

This gives the disjoint decomposition

$$\begin{aligned} F(\Lambda) &= \bigsqcup_{E\in P} \{h \in F(\Lambda) \mid E \text{ sign. matrix of } h \text{ w.r.t. } \Lambda\} \\ &= \bigsqcup_{E\in P} g(DGE^{-1} \cap G) = \bigsqcup_{E\in P} gH\sigma_E, \end{aligned}$$

of translated copies of the group H. Similarly we find

$$F(\Lambda_-, \Lambda_+) = \bigsqcup_{(E_-,E_+)\in Q} gT\sigma_{E_-^{-1}E_+}.$$

A consequence of the proof of Lemma 4.2.12 is that the groups H, H_-, H_+ have finite index in G and hence so does T. Therefore the groups H, T are μ-measurable with $\mu(H) = |G : H|^{-1} > 0$ and similarly for T. The Haar measure μ is translation invariant, so $\mu(H) = \mu(gH\sigma_E)$ and $\mu(T) = \mu(gT\sigma_{E_-^{-1}E_+})$. This gives

$$\mu(F(\Lambda)) = |P| \cdot \mu(H) \quad \text{and} \quad \mu(F(\Lambda_-, \Lambda_+)) = |Q| \cdot \mu(T).$$

Because we have $|P| = |Q|$, it remains to show that $\mu(H) = \mu(T)$ in order to prove $\mu(F(\Lambda)) = \mu(F(\Lambda_-, \Lambda_+))$.

We continue with the computation of $|G : H|, |G : T|$, making use of Lemma 4.2.13 and the notation introduced therein. For $i \in \mathbf{N}$ we use the abbreviation G_i for the i-th principal congruence subgroup $\mathrm{GL}_d^i(\mathcal{O})$ and we write q for the cardinality of the residue field of K. The lemma shows that each element of H can be conveniently described in terms of block matrices: the group H consists precisely of all matrices of the form

$$\begin{pmatrix} H_{11} & H_{12} & \dots & H_{1\ell} \\ H_{21} & H_{22} & & H_{2\ell} \\ \vdots & & \ddots & \vdots \\ H_{\ell 1} & H_{\ell 2} & \dots & H_{\ell\ell} \end{pmatrix}$$

with $H_{ii} \in \mathrm{GL}_{m_i}(\mathcal{O})$ for $1 \le i \le \ell$, $H_{ij} \in \pi^{a_i - a_j}\mathrm{Mat}_{m_i m_j}(\mathcal{O})$ for $1 \le j < i \le \ell$ and $H_{ij} \in \mathrm{Mat}_{m_i m_j}(\mathcal{O})$ for $1 \le i < j \le \ell$. This in turn shows that the group HG_1 consists precisely of all matrices of the form

$$\begin{pmatrix} A_{11} & A_{12} & \dots & A_{1\ell} \\ A_{21} & A_{22} & & A_{2\ell} \\ \vdots & & \ddots & \vdots \\ A_{\ell 1} & A_{\ell 2} & \dots & A_{\ell\ell} \end{pmatrix}$$

with $A_{ii} \in \mathrm{GL}_{m_i}(\mathcal{O})$ for $1 \le i \le \ell$, $A_{ij} \in \pi\mathrm{Mat}_{m_i m_j}(\mathcal{O})$ for $1 \le j < i \le \ell$ and $A_{ij} \in \mathrm{Mat}_{m_i m_j}(\mathcal{O})$ for $1 \le i < j \le \ell$. It follows that the index $|HG_1 : H|$ is given by

$$|HG_1 : H| = \prod_{1\le j<i\le \ell} q^{(a_i - a_j - 1)m_i m_j}. \tag{4.23}$$

Moreover, the group HG_1/G_1 consists precisely of all matrices of the form

$$\begin{pmatrix} B_{11} & B_{12} & \dots & B_{1\ell} \\ B_{21} & B_{22} & & B_{2\ell} \\ \vdots & & \ddots & \vdots \\ B_{\ell 1} & B_{\ell 2} & \dots & B_{\ell\ell} \end{pmatrix}$$

with $B_{ii} \in \mathrm{GL}_{m_i}(\mathbf{F}_q)$ for $1 \leq i \leq \ell$, $B_{ij} = 0 \in \mathrm{Mat}_{m_i m_j}(\mathbf{F}_q)$ for $1 \leq j < i \leq \ell$ and $B_{ij} \in \mathrm{Mat}_{m_i m_j}(\mathbf{F}_q)$ for $1 \leq i < j \leq \ell$. Therefore we have

$$|G : HG_1| = |G/G_1 : HG_1/G_1| = |\mathrm{GL}_d(\mathbf{F}_q)| \cdot \prod_{i=1}^{\ell} |\mathrm{GL}_{m_i}(\mathbf{F}_q)|^{-1} \cdot \prod_{1 \leq i < j \leq \ell} q^{-m_i m_j} \tag{4.24}$$

and combining this with equation (4.23) we get

$$\begin{aligned} |G : H| &= |G : HG_1||HG_1 : H| \\ &= |\mathrm{GL}_d(\mathbf{F}_q)| \prod_{i=1}^{\ell} |\mathrm{GL}_{m_i}(\mathbf{F}_q)|^{-1} \cdot \prod_{1 \leq i < j \leq \ell} q^{-m_i m_j} \cdot \prod_{1 \leq j < i \leq \ell} q^{(a_i - a_j - 1) m_i m_j}. \end{aligned} \tag{4.25}$$

Let k be the smallest positive integer i such that $a_i \geq 0$. If no such i exists, we set $k = \ell + 1$. Write $N = a_\ell - a_1 \geq 0$, if $N = 0$ then $D = \pi^e I$ for some $e \in \mathbf{Z}$ and hence $H = H_\pm = K = G$ so the lemma is true. Suppose $N > 0$, in the second part of the proof of Lemma 4.2.12 we showed that the congruence subgroup G_N is contained in the groups H_-, H_+ and hence also in the group $T = H_- \cap H_+$. We have

$$|G : T| = \frac{|G : G_N|}{|T : G_N|} = \frac{|\mathrm{GL}_d(\mathbf{F}_q)| q^{d^2(N-1)}}{|T : G_N|}, \tag{4.26}$$

so in order to compute $|G : T|$, it suffices to compute the index $|T : G_N|$. Lemma 4.2.13 gives us explicit descriptions of the groups H_-, H_+ in terms of block matrices; combining them we get the following description of T in terms of 7 (possibly degenerate) "regions" $T_0, T_1, \dots, T_6$ (T_0 is the diagonal region, T_1, T_2, T_3 are regions above the diagonal and T_4, T_5, T_6 are regions below the diagonal, the T_i are numbered clockwise).

Region	Description	Condition
T_0	$T_{ii} = \mathrm{GL}_{m_i}(\mathcal{O})$	$i = j$
T_1	$T_{ij} = \pi^{a_j - a_i}\mathrm{Mat}_{m_i m_j}(\mathcal{O})$	$i < j < k$
T_2	$T_{ij} = \pi^{-a_i}\mathrm{Mat}_{m_i m_j}(\mathcal{O})$	$i < k \leq j$
T_3	$T_{ij} = M_{m_i m_j}(\mathcal{O})$	$k \leq i < j$
T_4	$T_{ij} = \pi^{a_i - a_j}\mathrm{Mat}_{m_i m_j}(\mathcal{O})$	$k \leq j < i$
T_5	$T_{ij} = \pi^{a_i}\mathrm{Mat}_{m_i m_j}(\mathcal{O})$	$j < k \leq i$
T_6	$T_{ij} = \mathrm{Mat}_{m_i m_j}(\mathcal{O})$	$j < i < k$

$$\left(\begin{array}{cc|cc} \ddots & 1 & & 2 \\ 6 & \ddots & & \\ \hline & & \ddots & 3 \\ 5 & & 4 & \ddots \end{array}\right)$$

We will compute the contribution of each region T_i to $|T : G_N|$. We first combine the contributions of the regions T_5, T_2 modulo G_N, namely for $j < k \leq i$ the blocks T_{ij} and T_{ji} give a contribution of

$$(q^{N-a_i})^{m_i m_j} \cdot (q^{N+a_j})^{m_i m_j} = q^{(N-a_i+a_j)m_i m_j} \cdot q^{N m_i m_j}$$

and hence the regions T_2, T_5 together contribute

$$\prod_{j<k\leq i} q^{(N-a_i+a_j)m_i m_j} \cdot q^{N m_i m_j}.$$

The regions T_1 (consider T_{ji} for $j < i < k$), T_4 contribute

$$\prod_{j<i<k} q^{(N-a_i+a_j)m_i m_j} \cdot \prod_{k\leq j<i} q^{(N-a_i+a_j)m_i m_j}$$

to $|T : G_N|$ and hence the four regions T_1, T_2, T_4, T_5 together contribute

$$\prod_{j<i} q^{(N-a_i+a_j)m_i m_j} \cdot \prod_{j<k\leq i} q^{N m_i m_j}.$$

Lastly the regions T_3 (consider T_{ji} for $k \leq j < i$), T_6 give a contribution of

$$\prod_{k\leq j<i} q^{N m_i m_j} \cdot \prod_{j<i<k} q^{N m_i m_j}$$

and therefore the total contribution of the regions $T_1, \ldots, T_6$ is equal to

$$\prod_{j<i} q^{(N-a_i+a_j)m_i m_j} \cdot \prod_{j<i} q^{N m_i m_j}.$$

The region T_0 gives the contribution

$$\prod_{i=1}^{\ell} |\mathrm{GL}_{m_i}(\mathbf{F}_q)| q^{m_i^2(N-1)}$$

and hence

$$|T : G_N| = \prod_{i=1}^{\ell} |\mathrm{GL}_{m_i}(\mathbf{F}_q)| q^{m_i^2(N-1)} \cdot \prod_{1\leq j<i\leq \ell} q^{(N-a_i+a_j)m_i m_j} \cdot \prod_{1\leq j<i\leq \ell} q^{N m_i m_j}. \tag{4.27}$$

Combining the equations (4.25), (4.26) and (4.27) together with $d^2 = (\sum_{i=1}^{\ell} m_i)^2 = \sum_{i=1}^{\ell} m_i^2 + 2\sum_{1\leq j<i\leq \ell} m_i m_j$ shows that we have $|G : H| = |G : T|$.

□

Example 4.4.4. We illustrate with an example the second halve of the above proof of Theorem 4.4.3. Let p be a prime number and take $(K, \mathcal{O}) = (\mathbf{Q}_p, \mathbf{Z}_p)$. Write $G = \mathrm{GL}_5(\mathbf{Z}_p)$, $G_1 = \mathrm{GL}_5^1(\mathbf{Z}_p)$. For the signature matrix $D = \mathrm{diag}(p^{-1}, p^{-1}, p, p^2, p^2)$ we have

$$D_- = \mathrm{diag}(p, p, 1, 1, 1) \quad \text{and} \quad D_+ = \mathrm{diag}(1, 1, p, p^2, p^2).$$

Moreover we have $(e_1, \ldots, e_5) = (-1, -1, 1, 2, 2)$, $(a_1, a_2, a_3) = (-1, 1, 2)$, $(m_1, m_2, m_3) = (2, 1, 2)$. The group $H = G \cap DGD^{-1}$ is given by

$$H = \begin{pmatrix} \mathrm{GL}_2(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p & \mathbf{Z}_p \\ & \mathbf{Z}_p & \mathbf{Z}_p & \mathbf{Z}_p \\ p^2\mathbf{Z}_p \quad p^2\mathbf{Z}_p & \mathrm{GL}_1(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p \\ p^3\mathbf{Z}_p \quad p^3\mathbf{Z}_p & p\mathbf{Z}_p & \mathrm{GL}_2(\mathbf{Z}_p) & \\ p^3\mathbf{Z}_p \quad p^3\mathbf{Z}_p & p\mathbf{Z}_p & & \end{pmatrix}$$

and the groups $H_\pm = G \cap D_\pm G D_\pm^{-1}$ by

$$H_- = \begin{pmatrix} \mathrm{GL}_2(\mathbf{Z}_p) & p\mathbf{Z}_p & p\mathbf{Z}_p & p\mathbf{Z}_p \\ & p\mathbf{Z}_p & p\mathbf{Z}_p & p\mathbf{Z}_p \\ \mathbf{Z}_p \quad \mathbf{Z}_p & & & \\ \mathbf{Z}_p \quad \mathbf{Z}_p & & \mathrm{GL}_3(\mathbf{Z}_p) & \\ \mathbf{Z}_p \quad \mathbf{Z}_p & & & \end{pmatrix} \text{ and } H_+ = \begin{pmatrix} \mathrm{GL}_2(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p & \mathbf{Z}_p \\ & \mathbf{Z}_p & \mathbf{Z}_p & \mathbf{Z}_p \\ p\mathbf{Z}_p \quad p\mathbf{Z}_p & \mathrm{GL}_1(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p \\ p^2\mathbf{Z}_p \quad p^2\mathbf{Z}_p & p\mathbf{Z}_p & \mathrm{GL}_2(\mathbf{Z}_p) & \\ p^2\mathbf{Z}_p \quad p^2\mathbf{Z}_p & p\mathbf{Z}_p & & \end{pmatrix}.$$

Using the explicit form of H, we see that HG_1 and HG_1/G_1 are given by

$$HG_1 = \begin{pmatrix} \mathrm{GL}_2(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p & \mathbf{Z}_p \\ & \mathbf{Z}_p & \mathbf{Z}_p & \mathbf{Z}_p \\ p\mathbf{Z}_p \quad p\mathbf{Z}_p & \mathrm{GL}_1(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p \\ p\mathbf{Z}_p \quad p\mathbf{Z}_p & p\mathbf{Z}_p & \mathrm{GL}_2(\mathbf{Z}_p) & \\ p\mathbf{Z}_p \quad p\mathbf{Z}_p & p\mathbf{Z}_p & & \end{pmatrix},$$

and

$$HG_1/G_1 \cong \begin{pmatrix} \mathrm{GL}_2(\mathbf{F}_p) & \mathbf{F}_p & \mathbf{F}_p & \mathbf{F}_p \\ & \mathbf{F}_p & \mathbf{F}_p & \mathbf{F}_p \\ & \mathrm{GL}_1(\mathbf{F}_p) & \mathbf{F}_p & \mathbf{F}_p \\ & & & \mathrm{GL}_2(\mathbf{F}_p) \end{pmatrix},$$

hence $|HG_1 : H| = p^{10}$ and $|HG_1/G_1| = |\mathrm{GL}_2(\mathbf{F}_p)|^2 \cdot |\mathrm{GL}_1(\mathbf{F}_p)| \cdot p^8$.

4.5 Appendix

In this appendix we give two different approaches, as to the one given in Chapter 1, to compute the commensurability zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ for the pair of abelian groups $(\mathbf{Q}^d,\mathbf{Z}^d)$ when $d \in \{2,3\}$. Let p be a prime number. Both approaches make use of the existence of a (formal) Euler product for the commensurability zeta function (see [8, Proposition 1.2]), of which Theorem 4.1.4 is a generalisation, to reduce the problem to computing the zeta function $\zeta^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(s)$ for the pair $(\mathbf{Q}_p^d,\mathbf{Z}_p^d)$ of abelian groups. This latter zeta function encodes the commensurability index for $\mathbf{Z}_p$-lattices of $\mathbf{Q}_p^d$ of rank d and we are able to compute it using different techniques. It still remains a challenge to extend these methods to cover higher values of d.

The first method makes use of the existence of a standard form for bases of $\mathbf{Z}_p$-lattices in $\mathcal{L}(\mathbf{Q}_p^2)$, encoded as an element of $\mathrm{Mat}_2(\mathbf{Q}_p)$. The second method uses the affine Bruhat-Tits building of $\mathrm{GL}_d(\mathbf{Q}_p)$ as a guideline for streamlining the computation of the commensurability zeta function. Throughout the whole appendix, p will always denote a prime number and we will use the notation of Chapter 4, see also Chapter 2. Recall from Chapter 4 that

$$\zeta^{\mathrm{comm}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(s) = Z^{\mathrm{comm}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t) = \sum_{\Lambda\in\mathcal{L}(\mathbf{Q}_p^2)} t^{\widetilde{c}(\Lambda)} \quad \text{with } t = p^{-s}$$

and we write $v : \mathbf{Q}_p \to \mathbf{Z}\cup\{\infty\}$ for the standard valuation on $\mathbf{Q}_p$ with induced absolute value $|.|_p$, we set $|x|_p = p^{-v(x)}$ for $x \in \mathbf{Q}_p$.

4.5.1 Standard basis

We give an overview of computation of the commensurability zeta function $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(t)$ for $d = 2$ using the help of a standard basis. With this standard basis at hand it is a straightforward exercise to compute the commensurability index. Although applicable for $d > 2$, we do not see a way to do this without considering many case distinctions.

An element $A \in \mathrm{GL}_2(\mathbf{Z}_p)$ can be seen as an automorphism of the additive group $\mathbf{Q}_p^2$. The index $|\Gamma : \Gamma'|$ of two $\mathbf{Z}_p$-lattices $\Gamma,\Gamma' \in \mathcal{L}(\mathbf{Q}_p^2)$ with $\Gamma' \subseteq \Gamma$ therefore does not change under the linear map induced by A, i.e.

$$|\Gamma : \Gamma'| = |A\Gamma : A\Gamma'| \tag{4.28}$$

where $A\Gamma, A\Gamma'$ stand for the image of Γ,Γ' under the linear map A. This observation leads to the following two useful lemmas.

Lemma 4.5.1. *Let $A, B \in \mathrm{GL}_2(\mathbf{Q}_p)$ be two matrices whose columns span the $\mathbf{Z}_p$-lattices Λ and $\Lambda \cap \mathbf{Z}_p^2$ respectively, then*

$$c(\Lambda) = |\det(AB^{-2})|_p = p^{2v(\det(B))-v(\det(A))}.$$

Proof. We make use of the following well-known result: if $\Gamma \subseteq \mathbf{Z}_p^2$ is a $\mathbf{Z}_p$-lattice and $T \in \mathrm{GL}_2(\mathbf{Q}_p)$ a matrix whose columns span Γ, then $|\mathbf{Z}_p^2 : \Gamma| = |\det(T)|_p^{-1} = p^{v(\det(B))}$. This gives

$$\begin{aligned} c(\Lambda) &= |\Lambda : \Lambda \cap \mathbf{Z}_p^2||\mathbf{Z}_p^2 : \Lambda \cap \mathbf{Z}_p^2| = |A\mathbf{Z}_p^2 : B\mathbf{Z}_p^2||\mathbf{Z}_p^2 : B\mathbf{Z}_p^2| \\ &= |\mathbf{Z}_p^2 : A^{-1}B\mathbf{Z}_p^2||\mathbf{Z}_p^2 : B\mathbf{Z}_p^2| = p^{v(\det(A^{-1}B))} \cdot p^{v(\det(B))} \end{aligned}$$

using that the $\mathbf{Z}_p$-lattice $A^{-1}B\mathbf{Z}_p^2$ is spanned by the columns of $A^{-1}B$. □

Lemma 4.5.2. *Let $A \in \mathrm{GL}_2(\mathbf{Q}_p)$ be an invertible matrix and let Λ, Λ' be two $\mathbf{Z}_p$-lattices in $\mathcal{L}(\mathbf{Q}_p^2)$ spanned by the columns of A and A^{-1} respectively. We then have $c(\Lambda) = c(\Lambda')$.*

Proof. The lattice Λ is the image of $\mathbf{Z}_p^2$ under the linear map induced by A, i.e. $\Lambda = A\mathbf{Z}_p^2$ and similar for Λ'. We then have

$$|\Lambda' : \Lambda' \cap \mathbf{Z}_p^2| = |A^{-1}\mathbf{Z}_p^2 : A^{-1}\mathbf{Z}_p^2 \cap \mathbf{Z}_p^2| = |\mathbf{Z}_p^2 : \mathbf{Z}_p^2 \cap A\mathbf{Z}_p^2| = |\mathbf{Z}_p^2 : \Lambda \cap \mathbf{Z}_p^2|,$$

using observation (4.28) in the second equality, similarly $|\mathbf{Z}_p^2 : \Lambda' \cap \mathbf{Z}_p^2| = |\Lambda : \Lambda \cap \mathbf{Z}_p^2|$ and hence $c(\Lambda) = c(\Lambda')$. □

Remark 4.5.3. Lemma 4.5.2 follows immediately from Lemma 4.2.11 together with the remark that the signature matrix of Λ' is the inverse of the signature matrix of Λ.

To compute the commensurability index $\widetilde{c}(\Lambda)$ for every $\mathbf{Z}_p$-lattice $\Lambda \in \mathcal{L}(\mathbf{Q}_p^2)$ we introduce a standard form for bases of $\mathbf{Z}_p$-lattices in $\mathcal{L}(\mathbf{Q}_p^d)$. For a $\mathbf{Z}_p$-lattice $\Lambda \in \mathcal{L}(\mathbf{Q}_p^2)$ let $A \in \mathrm{GL}_2(\mathbf{Q}_p)$ be a matrix whose columns are a $\mathbf{Z}_p$-basis for Λ, then the set $A \cdot \mathrm{GL}_2(\mathbf{Z}_p) = \{AB \mid B \in \mathrm{GL}_2(\mathbf{Z}_p)\}$ consists of all matrices whose columns form a $\mathbf{Z}_p$-basis of Λ. Multiplying with an appropriate element from $\mathrm{GL}_2(\mathbf{Z}_p)$, we see that the matrix A can be assumed to be of the form

$$\begin{pmatrix} p^k & ap^\ell \\ 0 & p^m \end{pmatrix} \tag{4.29}$$

for integers $a, k, l, m \in \mathbf{Z}$. If we additionally assume, when $a \neq 0$, that $p \nmid a$, $\ell < k$ and $0 < a < p^{k-\ell}$, then the matrix in (4.29) is a standard form for $\mathbf{Z}_p$-lattices in $\mathbf{Q}_p^2$. This means that the columns of two different matrices in this standard form span different $\mathbf{Z}_p$-lattices and that every $\mathbf{Z}_p$-lattices of rank 2 in $\mathbf{Q}_p^2$ has the columns of a matrix of the form in (4.29) as a basis. In case $a \neq 0$ we have for fixed $k, \ell \in \mathbf{Z}$ precisely $(p-1)p^{k-\ell-1}$ possibilities for a.

Using this standard form of bases for lattices in $\mathcal{L}(\mathbf{Q}_p^2)$, we can compute the commensurability index by making use of a case distinction. For an overview see Table 4.1. Let A be the matrix in (4.29) and write Λ for the $\mathbf{Z}_p$-lattice spanned by the columns of A.

(i) Suppose that $a = 0$, then $A = \begin{pmatrix} p^k & 0 \\ 0 & p^m \end{pmatrix}$ and hence a basis of $\Lambda \cap \mathbf{Z}_p^2$ is given by the columns of the matrix $\begin{pmatrix} p^{\max\{0,k\}} & 0 \\ 0 & p^{\max\{0,m\}} \end{pmatrix}$. By Lemma 4.5.1 the commensurability index $c(\Lambda)$ is given by

$$c(\Lambda) = p^{2(\max\{0,k\}+\max\{0,m\})-(k+m)} = p^{|k|+|m|}.$$

When $a \neq 0$, we compute $A^{-1} = \begin{pmatrix} p^{-k} & -ap^{\ell-k-m} \\ 0 & p^{-m} \end{pmatrix}$. When $-k \leq \ell - k - m$ or equivalently $m \leq \ell$, we are in the situation of case (i). Write Λ' for the $\mathbf{Z}_p$-lattice spanned by the columns of A^{-1}.

(ii) Suppose $m \leq \ell$, then a basis for Λ' is given by the columns of the matrix $\begin{pmatrix} p^{-k} & 0 \\ 0 & p^{-m} \end{pmatrix}$. Making use of Lemma 4.5.2 we find

$$c(\Lambda) = c(\Lambda') = p^{|k|+|m|}.$$

From this point onwards we assume that $\ell < m$. We are going to make a case distinction which depends on the sign of k and ℓ.

(iii) Suppose $k \geq 0, \ell < 0$, then a basis for the lattice $\Lambda \cap \mathbf{Z}_p^2$ is given by the columns of the matrix $\begin{pmatrix} p^k & a \\ 0 & p^{m-\ell} \end{pmatrix}$. By Lemma 4.5.1 we find

$$c(\Lambda) = p^{2(k+m-\ell)-(k+m)} = p^{k+m-2\ell}.$$

(iv) Suppose $k, \ell \geq 0$, then $\Lambda \subseteq \mathbf{Z}_p^2$ and hence

$$c(\Lambda) = |\mathbf{Z}_p^2 : \Lambda| = p^{k+m}.$$

(v) & (vi) Suppose $k < 0$. Looking at A^{-1} we see that, depending on whether $\ell - k - m$ is strictly negative or nonnegative, we can use the cases (iii) and (iv) respectively to compute $c(\Lambda)$ with Lemma 4.5.2. This gives

$$c(\Lambda) = c(\Lambda') = \begin{cases} p^{k+m-2\ell} \text{ if } \ell - k - m < 0 \\ p^{-k-m} \text{ if } \ell - k - m \geq 0 \end{cases}.$$

The case distinction subdivides the computation of the commensurability zeta function $Z^{\text{comm}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t)$ into 6 different parts. Namely $Z^{\text{comm, (i)}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t), \ldots, Z^{\text{comm, (vi)}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t)$, according to the cases (i)-(vi). In each case we know the formula for the commensurability index, so we only need to sum over all possible standard forms in every fixed case to compute the contribution to $Z^{\text{comm}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t)$. A quick look shows that each of these contributions is a combination of iterated geometric sums and therefore straightforward to compute. As an example we compute the zeta functions $Z^{\text{comm,(i)}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t)$, $Z^{\text{comm, (iii)}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t)$ and leave the others to the reader.

Case	Conditions	$c(\Lambda)$
(i)	$a = 0$	$p^{\lvert k\rvert+\lvert m\rvert}$
(ii)	$m \leq \ell < k$	$p^{\lvert k\rvert+\lvert m\rvert}$
(iii)	$k \geq 0, \ell < 0$ $\ell < k, m$	$p^{k+m-2\ell}$
(iv)	$k, \ell \geq 0$ $\ell < k, m$	p^{k+m}
(v)	$k < 0, \ell < k, m$ $\ell < k + m$	$p^{k+m-2\ell}$
(vi)	$k < 0, \ell < k, m$ $\ell \geq k + m$	p^{-k-m}

Table 4.1: Overview of the case distinction.

- Case (i) gives the contribution

$$Z^{\text{comm, (i)}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t) = \sum_{k,m\in\mathbf{Z}} \left(p^{|k|+|m|}\right)^{-s} = \left(\sum_{k\in\mathbf{Z}} p^{-|k|s}\right)^2$$
$$= \left(1 + 2\sum_{k=1}^{\infty} p^{-ks}\right)^2 = \frac{(1+p^{-s})^2}{(1-p^{-s})^2}.$$

- The case (iii) gives the contribution $Z^{\text{comm, (iii)}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t)$, which equals

$$\sum_{\substack{k\geq 0,\ell<0\\ \ell<k,m}} (p-1)p^{k-\ell-1}\left(p^{k+m-2\ell}\right)^{-s} = \frac{p-1}{p}\left(\sum_{k=0}^{\infty} p^{k(1-s)}\right)\left(\sum_{\ell<0} p^{-(1-2s)\ell}\sum_{m>\ell} p^{-ms}\right)$$
$$= \frac{p-1}{p}\cdot\frac{1}{1-p^{1-s}}\left(\sum_{\ell<0} p^{-(1-2s)\ell}\cdot\frac{p^{-(\ell+1)s}}{1-p^{-s}}\right)$$
$$= \frac{(p-1)p^{-s}}{p(1-p^{1-s})(1-p^{-s})}\left(\sum_{\ell<0} p^{-(1-s)\ell}\right)$$
$$= \frac{(p-1)p^{-2s}}{(1-p^{1-s})(1-p^{-s})}.$$

Calculating the contributions of the other cases and addding them up shows that

$$\zeta^{\text{comm}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(s) = \frac{(1-p^{-2s})(1-p^{1-2s})}{(1-p^{-s})^2(1-p^{1-s})^2},$$

which agrees with the local factor at p of of the zeta function $\zeta^{\text{comm}}_{\mathbf{Q}^d,\mathbf{Z}^d}(s)$ in Corollary 4.1.2.

4.5.2 Buildings

Using the (Bruhat-Tits) building of $\mathrm{GL}_d(\mathbf{Q}_p)$ for $d \in \{2,3\}$ we compute the commensurability zeta function $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(t)$. The same method can be used when $d > 3$, but this becomes more challenging, because we do not know how to simplify the complicated formulas in a structured way to end up with a reduced expression for $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(t)$. Already for the case $d = 3$ this happens. The computation is not limited to the field $\mathbf{Q}_p$, it works for any non-Archimedean local field K, because the concept of buildings extends to $\mathrm{GL}_d(K)$ as well. As this section is only for exposition, we stick to the field $\mathbf{Q}_p$.

First we give a short overview of the Bruhat-Tits building of $\mathrm{GL}_d(\mathbf{Q}_p)$, followed by an outline of the computation. We subdivide the computation into several smaller parts and after solving each of them we put everything together and compute the zeta function.

Building of $\mathbf{GL}_d(\mathbf{Q}_p)$

We give a short overview of the Bruhat-Tits building of the group $\mathrm{GL}_d(\mathbf{Q}_p)$, and some relevant results. For details and proofs, see for example [59], Chapter II §1. Define an equivalence relation on the set $\mathcal{L}(\mathbf{Q}_p^d)$ of all $\mathbf{Z}_p$-lattices of $\mathbf{Q}_p^d$ of rank d. Two $\mathbf{Z}_p$-lattices $\Lambda, \Gamma \in \mathcal{L}(\mathbf{Q}_p^d)$ are equivalent, if there exists an integer $k \in \mathbf{Z}$ such that $\Gamma = p^k\Lambda$ (i.e. Λ, Γ are up to homothety the same). We denote the equivalence class of $\Lambda \in \mathcal{L}(\mathbf{Q}_p^d)$ by $[\Lambda]$. The building $X = X(p,d)$ of $\mathrm{GL}_d(\mathbf{Q}_p)$ is a simplicial complex, whose 0-simplices (vertices) are the equivalence classes $[\Lambda]$ for $\Lambda \in \mathcal{L}(\mathbf{Q}_p^d)$. Let $1 \leq k \leq d$ be an integer, the vertices $v_0, \ldots, v_{k-1}$ of X form a $(k-1)$-simplex, if there exist $\mathbf{Z}_p$-lattices $\Lambda_i \in \mathcal{L}(\mathbf{Q}_p^d)$ with $v_i = [\Lambda_i]$ satisfying

$$p\Lambda_0 \subsetneq \Lambda_{k-1} \subsetneq \ldots \subsetneq \Lambda_1 \subsetneq \Lambda_0.$$

The building X comes with a natural action of the group $\mathrm{GL}_d(\mathbf{Q}_p)$. The action of an element $g \in \mathrm{GL}_d(\mathbf{Q}_p)$ on a vertex $v \in X$ is defined by

$$g.v = [g\Lambda],$$

here $\Lambda \in \mathcal{L}(\mathbf{Q}_p^d)$ is a representative for the equivalence class v. This definition does not depend on choice of representative Λ. One can show that the action of $\mathrm{GL}_d(\mathbf{Q}_p)$ on X is transitive: for two sets of vertices $\{v_0, \ldots, v_{k-1}\}$ and $\{w_0, \ldots, w_{k-1}\}$ of X forming $(k-1)$-simplices there exists a $g \in \mathrm{GL}_d(\mathbf{Q}_p)$ such that $g.v_i = w_i$ for $0 \leq i \leq k-1$. Any subgroup of $\mathrm{GL}_d(\mathbf{Q}_p)$ acts naturally on X through the action of $\mathrm{GL}_d(\mathbf{Q}_p)$ on X.

Every vertex $v \in X$ has a unique representative $\mathbf{Z}_p$-lattice $\Lambda_v \in \mathcal{L}(\mathbf{Q}_p^d)$ satisfying $\Lambda_v \subseteq \mathbf{Z}_p^d$ and $\Lambda_v \subsetneq p\mathbf{Z}_p^d$. We call Λ_v the minimal lattice of v. Write $D_v = \mathrm{diag}(p^{e_1}, \ldots, p^{e_d})$, with $e_i \in \mathbf{Z}$, for a signature matrix of Λ_v (see Definition 4.2.3). Without loss of generality

we may assume that $e_1 \leq \ldots \leq e_d$, in this case we say that $(e_1, \ldots, e_d)$ is the signature of the vertex v. By definition of Λ_v we always have $e_1 = 0$.

Example 4.5.4. For $d = 2$ the description of the building X of $\mathrm{GL}_2(\mathbf{Q}_p)$ is surprisingly simple, which is largely due to the fact that X is a graph (undirected and no loops). The building X is a connected tree (also called the Bruhat-Tits tree) with each vertex having exactly $p+1$ neighbours. Two vertices $v_0, v_1 \in X$ are connected by an edge, if there exist representative $\mathbf{Z}_p$-lattices Λ_0, Λ_1 of respectively v_0, v_1 satisfying

$$p\Lambda_0 \subsetneq \Lambda_1 \subsetneq \Lambda_0.$$

One can describe the action of the group $\mathrm{GL}_2(\mathbf{Z}_p)$ on X as follows. The vertex $[\mathbf{Z}_p^2]$ is fixed by $\mathrm{GL}_2(\mathbf{Z}_p)$ and $\mathrm{GL}_2(\mathbf{Z}_p)$ acts transitive on the vertices of X with a given fixed distance from $[\mathbf{Z}_p^2]$. One could say that $\mathrm{GL}_2(\mathbf{Z}_p)$ acts by rotation on X.

For the computation of the commensurability zeta function $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t)$ for the pair $(\mathbf{Q}_p^d, \mathbf{Z}_p^d)$ of abelian groups we only need the 0-simplices and the 1-simplices of X, i.e. the 1-skeleton (or underlying graph) of X.

Outline of the computation

The combinatorial structure of the building X of $\mathrm{GL}_d(\mathbf{Q}_p)$ allows us to break up the computation of $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t)$ into smaller, more managable parts. From the construction of the building X we see immediately that

$$Z^{\mathrm{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t) = \sum_{\Lambda \in \mathcal{L}(\mathbf{Q}_p^d)} t^{\widetilde{c}(\Lambda)} = \sum_{v \in X} \sum_{\Lambda \text{ s.t. } v = [\Lambda]} t^{\widetilde{c}(\Lambda)},$$

where in the double summation we first sum over all vertices v of X and then, for a fixed vertex v, over all $\mathbf{Z}_p$-lattices $\Lambda \in \mathcal{L}(\mathbf{Q}_p^d)$ belonging to the equivalence class v. For a $\mathbf{Z}_p$-lattice $\Lambda \in \mathcal{L}(\mathbf{Q}_p^d)$ and $g \in \mathrm{GL}_d(\mathbf{Z}_p)$ we have

$$\begin{aligned} c(g\Lambda) &= |g\Lambda : g\Lambda \cap \mathbf{Z}_p^d||\mathbf{Z}_p^d : g\Lambda \cap \mathbf{Z}_p^d| \\ &= |\Lambda : \Lambda \cap g^{-1}\mathbf{Z}_p^d||g^{-1}\mathbf{Z}_p^d : \Lambda \cap g^{-1}\mathbf{Z}_p^d| = c(\Lambda), \end{aligned}$$

where we used for the last equation that $g^{-1}\mathbf{Z}_p^d = \mathbf{Z}_p^d$. This shows that the commensurability index is invariant under the left action of $\mathrm{GL}_d(\mathbf{Z}_p)$. Two vertices $v, w \in X$ lying in the same orbit of the action of $\mathrm{GL}_d(\mathbf{Z}_p)$ give the same contributions to $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t)$. Grouping together those vertices belonging to the same orbit of $\mathrm{GL}_d(\mathbf{Z}_p)$ gives the formula

$$Z^{\mathrm{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t) = \sum_{\mathrm{GL}_d(\mathbf{Z}_p).v \in \mathrm{GL}_d(\mathbf{Z}_p)\backslash X} |\mathrm{GL}_d(\mathbf{Z}_p).v| \sum_{\Lambda \text{ s.t. } v = [\Lambda]} t^{\widetilde{c}(\Lambda)},$$

here the first summation runs over all orbits $\mathrm{GL}_d(\mathbf{Z}_p)\backslash X$ of the action of $\mathrm{GL}_d(\mathbf{Z}_p)$ on X and, for an orbit $\mathrm{GL}_d(\mathbf{Z}_p).v$ with a $v \in X$ a vertex, we write $|\mathrm{GL}_d(\mathbf{Z}_p).v|$ for the size of the orbit $\mathrm{GL}_d(\mathbf{Z}_p).v$. Answering the following three questions to a sufficient degree, allows us to compute $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(t)$.

(1) Can we parametrise $\mathrm{GL}_d(\mathbf{Z}_p)\backslash X$?

(2) For a vertex $v \in X$, what is the cardinality of $\mathrm{GL}_d(\mathbf{Z}_p).v$?

(3) For a vertex $v \in X$, can we compute the sum $\sum_{\Lambda \text{ s.t. } v=[\Lambda]} t^{\widetilde{c}(\Lambda)}$?

The quotient space $\mathbf{GL}_d(\mathbf{Z}_p)\backslash X$

We make the following observation.

Lemma 4.5.5. *Two vertices $v, w \in X$ are in the same orbit under the action of $\mathrm{GL}_d(\mathbf{Z}_p)$ on X if and only if v and w have the same signatures.*

Proof. Let D_v, D_w be the signature matrices of Λ_v, Λ_w and let $g_v, g_w \in \mathrm{GL}_d(\mathbf{Z}_p)$ be elements such that $\Lambda_v = g_v D_v \mathbf{Z}_p^d$ and $\Lambda_w = g_w D_w \mathbf{Z}_p^d$. Suppose there exists an element $g \in \mathrm{GL}_d(\mathbf{Z}_p)$ such that $g.v = w$, then by uniqueness of the minimal lattice we have $g\Lambda_v = \Lambda_w$ and hence we can find an element $h \in \mathrm{GL}_d(\mathbf{Z}_p)$ such that

$$g g_v D_v = g_w D_w h.$$

The uniqueness part of Theorem 4.2.7 gives $D_v = D_w$. On the other hand, if the signatures of v and w are the same, then $g_w g_v^{-1}.v = w$ and hence v, w lie in the same orbit. □

It follows from Lemma 4.5.5 that we can paramatrise the orbit space $\mathrm{GL}_d(\mathbf{Z}_p)\backslash X$ by

$$\{(e_1, \ldots, e_d) \in \mathbf{Z}^d \mid 0 = e_1 \leq \ldots \leq e_d\}$$

and in particular the equivalence classes of the $\mathbf{Z}_p$-lattices $\mathrm{diag}(p^{e_1}, \ldots, p^{e_d})\mathbf{Z}_p^d$ with $0 = e_1 \leq \ldots \leq e_d$ form a full set of representatives of the orbit space $\mathrm{GL}_d(\mathbf{Z}_p)\backslash X$. This answers the first question.

We use the abbreviation G for the group $\mathrm{GL}_d(\mathbf{Z}_p)$ and for $i \in \mathbf{N}$ we write G_i for the i-th principal congruence subgroup

$$G_i = \ker(\mathrm{GL}_d(\mathbf{Z}_p) \to \mathrm{GL}_d(\mathbf{Z}/p^i\mathbf{Z})).$$

It is a well-known fact that the reduction map to $\mathrm{GL}_d(\mathbf{Z}_p/p^i\mathbf{Z}_p)$ is surjective, hence $G/G_i \cong \mathrm{GL}_d(\mathbf{Z}/p^i\mathbf{Z})$ and $|G : G_i| = |\mathrm{GL}_d(\mathbf{Z}/p^i\mathbf{Z})|$. The next lemma determines the sizes of the orbits of $\mathrm{GL}_d(\mathbf{Z}_p)$ on X, it is almost and immediate consequence of Lemma 4.2.12.

Proposition 4.5.6. *Let $v \in X$ be a vertex and $D = D_v$ a signature matrix of Λ_v, then*

$$|G.v| = |G : G \cap DGD^{-1}|.$$

Proof. By Lemma 4.5.5 the size of the orbit $G.v$ equals the number of lattices in $\mathcal{L}(\mathbf{Q}_p^d)$ having signature matrix D. By the proof of Lemma 4.2.12 this number equals $|G : G \cap DGD^{-1}|$. □

It is now an exercise to determine the sizes of the orbits of the action of $\mathrm{GL}_d(\mathbf{Z}_p)$ on X. We do this explicitly for $d \in \{2, 3\}$ using Lemma 4.2.13. Suppose $d = 2$, then there are two possibilities for the signature of a vertex $v \in X$: either $(0, 0)$ or $(0, \ell)$ for some integer $\ell > 0$.

- $(0, 0)$. In this case we have $D = I$ and hence there is just one orbit.
- $(0, \ell)$. Write $D = \left(\begin{smallmatrix} 1 & \\ & p^\ell \end{smallmatrix}\right)$, then we have $G_D = G \cap DGD^{-1} = \left(\begin{smallmatrix} \mathbf{Z}_p^* & \mathbf{Z}_p \\ p^\ell\mathbf{Z}_p & \mathbf{Z}_p^* \end{smallmatrix}\right)$. Since G_ℓ is a subgroup of G_D with $G_D/G_\ell \cong \left(\begin{smallmatrix} (\mathbf{Z}/p^\ell\mathbf{Z})^* & \mathbf{Z}/p^\ell\mathbf{Z} \\ & (\mathbf{Z}/p^\ell\mathbf{Z})^* \end{smallmatrix}\right)$, we have

$$\begin{aligned} |G.v| = |G : G_D| = \frac{|G : G_\ell|}{|G_D : G_\ell|} &= \frac{|\mathrm{GL}_2(\mathbf{Z}/p^\ell\mathbf{Z})|}{|\mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z})|^2 \cdot |\mathbf{Z}/p^\ell\mathbf{Z}|} \\ &= \frac{(p^2-1)(p^2-p)(p^{\ell-1})^4}{(p-1)^2 p^{3\ell-2}} = (p+1)p^{\ell-1}. \end{aligned}$$

  Which is also the size of the projective space $\mathbf{P}^1(\mathbf{Z}_p/p^\ell\mathbf{Z}_p) = (\mathbf{Z}_p^2 \backslash p^\ell\mathbf{Z}_p^2)/\mathbf{Z}_p^*$ and the number of vertices in X of distance ℓ to the vertex $[\mathbf{Z}_p^2]$. This is no coincidence, because there is a bijection between the two sets, given by

$$\mathbf{P}^1(\mathbf{Z}_p/p^\ell\mathbf{Z}_p) \ni [\lambda] \mapsto [p^\ell\mathbf{Z}_p^2 + \lambda\mathbf{Z}_p].$$

For $d = 3$ there are four possibilities for the signature of a vertex $v \in X$, it equals either $(0, 0, 0)$, $(0, 0, \ell)$ with $\ell > 0$, $(0, \ell, \ell)$ with $\ell > 0$ or $(0, k, \ell)$ with $0 < k < \ell$.

- $(0, 0, 0)$. In this case we have $D = I$ and hence there is just one orbit.
- $(0, 0, \ell)$ and $(0, \ell, \ell)$ with $\ell > 0$. The case $(0, \ell, \ell)$ goes analogously to $(0, 0, \ell)$ with the same result, so we consider only the case $(0, 0, \ell)$. Write $D = \mathrm{diag}(1, 1, p^\ell)$ and set $G_D = G \cap GDG^{-1}$, one computes

$$G_D = \begin{pmatrix} \mathrm{GL}_2(\mathbf{Z}_p) & \mathbf{Z}_p \\ p^\ell\mathbf{Z}_p \quad p^\ell\mathbf{Z}_p & \mathbf{Z}_p^* \end{pmatrix} \quad \text{and} \quad G_D/G_\ell \cong \begin{pmatrix} \mathrm{GL}_2(\mathbf{Z}/p^\ell\mathbf{Z}) & \mathbf{Z}/p^\ell\mathbf{Z} \\ & \mathbf{Z}/p^\ell\mathbf{Z} \\ & \mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z}) \end{pmatrix}.$$

Using the same method as for $d = 2$, we find

$$|G.v| = \frac{|\mathrm{GL}_3(\mathbf{Z}/p^\ell\mathbf{Z})|}{|\mathrm{GL}_2(\mathbf{Z}/p^\ell\mathbf{Z})||\mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z})||\mathbf{Z}/p^\ell\mathbf{Z}|^2} = (p^2+p+1)p^{2\ell-2}. \tag{4.30}$$

Which is also the size of the set $\mathbf{P}^2(\mathbf{Z}_p/p^\ell\mathbf{Z}_p)$.

- $(0,k,\ell)$ with $0 < k < \ell$. Write $D = \mathrm{diag}(1, p^k, p^\ell)$ and $G_D = G \cap DGD^{-1}$, one computes

$$G_D = \begin{pmatrix} \mathrm{GL}_1(\mathbf{Z}_p) & \mathbf{Z}_p & \mathbf{Z}_p \\ p^k\mathbf{Z}_p & \mathrm{GL}_1(\mathbf{Z}_p) & \mathbf{Z}_p \\ p^\ell\mathbf{Z}_p & p^{\ell-k}\mathbf{Z}_p & \mathrm{GL}_1(\mathbf{Z}_p) \end{pmatrix}$$

and

$$G_D/G_\ell \cong \begin{pmatrix} \mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z}) & \mathbf{Z}/p^\ell\mathbf{Z} & \mathbf{Z}/p^\ell\mathbf{Z} \\ p^k\mathbf{Z}/p^\ell\mathbf{Z} & \mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z}) & \mathbf{Z}/p^\ell\mathbf{Z} \\ & p^{\ell-k}\mathbf{Z}/p^\ell\mathbf{Z} & \mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z}) \end{pmatrix}.$$

Similarly to $d = 2$ this gives

$$|G.v| = \frac{|\mathrm{GL}_3(\mathbf{Z}/p^\ell\mathbf{Z})|}{|\mathrm{GL}_1(\mathbf{Z}/p^\ell\mathbf{Z})|^3 p^{4\ell}} = (p^2+p+1)(p+1)p^{2\ell-3}. \tag{4.31}$$

Note that the size of $G.v$ for the signature $(0,k,\ell)$ only depends on ℓ and not on the value of k!

The index $c(\Lambda)$ for homothetic lattices

We saw that the orbit space $\mathrm{GL}_d(\mathbf{Z}_p)\backslash X$ can be parametrised by tuples

$$\{(e_1, \ldots, e_d) \in \mathbf{Z}^d \mid 0 = e_1 \leq \ldots \leq e_d\},$$

where each such tuple $(e_1, \ldots, e_d)$ corresponds to the orbit $\mathrm{GL}_d(\mathbf{Z}_p).[\Lambda]$ for the $\mathbf{Z}_p$-lattice $\Lambda = \mathrm{diag}(p^{e_1}, \ldots, p^{e_d})\mathbf{Z}_p^d$. We will compute for this $\mathbf{Z}_p$-lattice Λ the contribution of the vertex $[\Lambda]$ to $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t)$, which is given by

$$\sum_{m \in \mathbf{Z}} t^{\widetilde{c}(p^m\Lambda)} = \sum_{m \in \mathbf{Z}} t^{|m+e_1|+\ldots+|m+e_d|}, \tag{4.32}$$

noting that any $\mathbf{Z}_p$-lattice in the equivalence class $[\Lambda]$ is of the form $p^m\Lambda$ for some integer $m \in \mathbf{Z}$ and that by Lemma (4.2.11) the commensurability index of $p^m\Lambda$ is

$$\widetilde{c}(p^m\Lambda) = |m+e_1| + \ldots + |m+e_d|.$$

Therefore we need to understand the function $m \mapsto \sum_{i=1}^d |m+e_i|$. Allowing m to take on real values, the graph of this function is a piecewise linear graph (i.e. the graph is a finite

union of line segments) and is, up to a vertical translation, determined by the inflection points (i.e. points where the slope changes). The m-coordinates of these inflection points are precisely those contained in the set $\{-e_1, \ldots, -e_d\}$.

The idea to compute the sum in (4.32) is to consider each piecewise linear part of the graph $m \mapsto \sum_{i=1}^{d} |m + e_i|$ separately and then combine each part. We do this explicitly for the cases $d \in \{2, 3\}$.

We consider first the case $d = 2$, then there are two different types of signatures: $(0, 0)$ or $(0, \ell)$ with $\ell > 0$.

- $(0, 0)$. We have $\widetilde{c}(p^m \Lambda) = 2|m|$ and

$$\sum_{m \in \mathbf{Z}} t^{2|m|} = 1 + 2 \sum_{m \geq 1} t^{2m} = \frac{1 + t^2}{1 - t^2}. \tag{4.33}$$

- $(0, \ell)$. The graph $m \mapsto |m| + |m + \ell|$ consists of three lines, from left to right they have respectively the slopes $-2, 0, 2$ and the inflection points are $(-\ell, \ell)$ and $(0, \ell)$. The contribution for $m \in \{-\ell + 1, \ldots, -1\}$ (the horizontal line) is given by $(\ell - 1)t^\ell$ (zero for $\ell = 1$). For $m \geq 0$ and $m \leq -\ell$ we get a contribution of respectively

$$\sum_{m \geq 0} t^{2m + \ell} = \frac{t^\ell}{1 - t^2} \quad \text{and} \quad \sum_{m \leq -\ell} t^{-2m - \ell} = \sum_{n \geq 0} t^{2n + \ell} = \frac{t^\ell}{1 - t^2}.$$

  It follows that

$$\sum_{m \in \mathbf{Z}} t^{|m| + |m + \ell|} = (\ell - 1)t^\ell + \frac{2t^\ell}{1 - t^2}. \tag{4.34}$$

Next we deal with the case $d = 3$, then the signatures come in four different types: $(0, 0, 0)$, $(0, 0, \ell)$ with $\ell > 0$, $(0, \ell, \ell)$ with $\ell > 0$ or $(0, k, \ell)$ with $0 < k < \ell$.

- $(0, 0, 0)$. We have $\widetilde{c}(p^m \Lambda) = 3|m|$ and

$$\sum_{m \in \mathbf{Z}} t^{3|m|} = 1 + 2 \sum_{m \geq 1} t^{3m} = \frac{1 + t^3}{1 - t^3}. \tag{4.35}$$

- $(0, 0, \ell)$. The graph $m \mapsto 2|m| + |m + \ell|$ consists of three lines, from left to right they have respectively the slopes $-3, -1, 3$ and the inflection points are $(-\ell, 2\ell)$ and $(0, \ell)$. The contribution for $m \in \{-\ell + 1, \ldots, -1\}$ (slope is -1) is given by

$$t^{\ell + 1} + \ldots + t^{2\ell - 1} = \frac{t^{\ell + 1} - t^{2\ell}}{1 - t}$$

(note that this is zero for $\ell = 1$, as it should be). For $m \geq 0$ and $m \leq -\ell$ we get a contribution of respectively

$$\sum_{m \geq 0} t^{3m+\ell} = \frac{t^\ell}{1-t^3} \quad \text{and} \quad \sum_{m \leq -\ell} t^{-3m-\ell} = \sum_{n \geq 0} t^{3n+2\ell} = \frac{t^{2\ell}}{1-t^3}.$$

So the total contribution is given by

$$\sum_{m \in \mathbf{Z}} t^{2|m|+|m+\ell|} = \frac{t^\ell + t^{2\ell}}{1-t^3} + \frac{t^{\ell+1} - t^{2\ell}}{1-t} \tag{4.36}$$

- $(0, \ell, \ell)$. The graph $m \mapsto |m| + 2|m+\ell|$ is up to a reflection in the vertical line $m = -\frac{1}{2}\ell$ the same as the one for $(0, 0, \ell)$ and hence its contribution is as well.
- $(0, k, \ell)$ with $0 < k < \ell$. The graph $m \mapsto |m| + |m+k| + |m+\ell|$ consists of four lines, from left to right they have respectively the slopes $-3, -1, 1, 3$ and the inflection points are $(-\ell, 2\ell - k)$, $(-k, \ell)$ and $(0, k+\ell)$. The contributions for $m \in \{-(k-1), \ldots, -1\}$ and $m \in \{-(\ell-1), \ldots, -k\}$ are given by respectively

$$t^{\ell+1} + \ldots + t^{k+\ell-1} = \frac{t^{\ell+1} - t^{k+\ell}}{1-t} \tag{4.37}$$

(for $k = 1$ this is zero, as it should be) and

$$t^\ell + \ldots + t^{2\ell-k-1} = \frac{t^\ell - t^{2\ell-k}}{1-t}.$$

For $m \geq 0$ and $m \leq -\ell$ we get a contribution of

$$\sum_{m \geq 0} t^{3m+k+\ell} = \frac{t^{k+\ell}}{1-t^3} \quad \text{and} \quad \sum_{m \leq -\ell} t^{-3m-k-\ell} = \sum_{n \geq 0} t^{3n+2\ell-k} = \frac{t^{2\ell-k}}{1-t^3}.$$

So the total contribution is given by

$$\sum_{m \in \mathbf{Z}} t^{|m|+|m+k|+|m+\ell|} = \frac{t^{k+\ell} + t^{2\ell-k}}{1-t^3} + \frac{t^{\ell+1} - t^{k+\ell}}{1-t} + \frac{t^\ell - t^{2\ell-k}}{1-t}.$$

The computation of the commensurability zeta function

We are now ready to compute the commensurability zeta function $Z^{\text{comm}}_{\mathbf{Q}_p^d, \mathbf{Z}_p^d}(t)$ for $d \in \{2, 3\}$. We start with the case $d = 2$. Let v be a vertex with signature $(0, 0)$ or $(0, \ell)$ for some $\ell > 0$, then the size of the orbit $\mathrm{GL}_d(\mathbf{Z}_p).v$ is respectively 1 or $(p+1)p^{\ell-1}$ and its contribution

to the commensurability zeta function is given in equation (4.33) or (4.34) respectively. It follows that the commensurability zeta function $Z^{\mathrm{comm}}_{\mathbf{Q}_p^d,\mathbf{Z}_p^d}(t)$ is given by

$$\begin{aligned} Z^{\mathrm{comm}}_{\mathbf{Q}_p^2,\mathbf{Z}_p^2}(t) &= \frac{1+t^2}{1-t^2} + \sum_{\ell>0}(p+1)p^{\ell-1}\left((\ell-1)t^\ell + \frac{2t^\ell}{1-t^2}\right) \\ &= \frac{1+t^2}{1-t^2} + (p+1)t\sum_{\ell>0}(\ell-1)(pt)^{\ell-1} + \frac{2(p+1)t}{1-t^2}\sum_{\ell>0}(pt)^{\ell-1} \\ &= \frac{1+t^2}{1-t^2} + \frac{(p^2+p)t^2}{(1-pt)^2} + \frac{2(p+1)t}{(1-t^2)(1-pt)} = \frac{(1-t^2)(1-pt^2)}{(1-t^2)(1-pt)^2}, \end{aligned}$$

using the formal identity $\sum_{k>0}(k-1)x^{k-1} = \frac{x}{(1-x)^2}$ in $\mathbf{Q}(\!(x)\!)$.

For the case $d=3$ the computation is more involved. We start by noting the identity

$$\sum_{k>0}\sum_{\ell>k} p^{a\ell}t^{b\ell+ck} = \sum_{k>0} t^{ck}\sum_{\ell>k}(p^at^b)^\ell = \frac{p^at^b}{1-p^at^b}\sum_{k>0}(p^at^{b+c})^k = \frac{p^{2a}t^{2b+c}}{(1-p^at^b)(1-p^at^{b+c})}$$

for $a,b,c\in\mathbf{Z}$ and we abbreviate this expression by $f(a,b,c)$. For a fixed $\ell>0$ the contribution of all vertices of the building of $\mathrm{GL}_3(\mathbf{Q}_p)$ with signature $(0,0,\ell)$ to the commensurability zeta function can be computed by combining (4.30) and (4.36), this contribution then equals

$$\sum_{\ell>0}(p^2+p+1)p^{2\ell-2}\left(\frac{t^\ell+t^{2\ell}}{1-t^3} + \frac{t^{\ell+1}-t^{2\ell}}{1-t}\right) \tag{4.38}$$

and, after some rewriting with geometric series, simplifies to

$$\frac{p^2+p+1}{p^2}\left(\frac{p^2t}{1-t^3}\left(\frac{1}{1-p^2t} + \frac{t}{1-p^2t^2}\right) + \frac{p^4t^3}{(1-p^2t)(1-p^2t^2)}\right).$$

For fixed $k,\ell\in\mathbf{Z}$ with $0<k<\ell$ the contribution of all vertices of the building of $\mathrm{GL}_3(\mathbf{Q}_p)$ with signature $(0,k,\ell)$ to the commensurability zeta function can be computed by combining (4.31) and (4.37), this contribution then equals

$$\sum_{k>0}\sum_{\ell>k}(p^2+p+1)(p+1)p^{2\ell-3}\left(\frac{t^{k+\ell}+t^{2\ell-k}}{1-t^3} + \frac{t^{\ell+1}-t^{k+\ell}}{1-t} + \frac{t^\ell - t^{2\ell-k}}{1-t}\right)$$

and simplifies to

$$\frac{(p^2+p+1)(p+1)}{p^3}\sum_{k>0}\sum_{\ell>k}p^{2\ell}\left(\frac{t^2+t}{t^3-1}(t^{k+\ell}+t^{2\ell-k}) + \frac{1+t}{1-t}t^\ell\right).$$

Using the expression for $f(a,b,c)$ in (4.38) and noting that $f(2,1,1) = f(2,2,-1)$, we see that the above sum equals

$$\frac{(p^2+p+1)(p+1)}{p^3}\left(\frac{t^2+t}{t^3-1}(f(2,1,1)+f(2,2,-1)) + \frac{1+t}{1-t}f(2,1,0)\right)$$

and hence evaluates to

$$\frac{(p^2+p+1)(p+1)}{p^3}\left(\frac{t^2+t}{t^3-1}\cdot\frac{2p^4t^3}{(1-p^2t)(1-p^2t^2)}+\frac{1+t}{1-t}\cdot\frac{p^4t^2}{(1-p^2t)^2}\right).$$

For a vertex with signature $(0,0,0)$ its contribution to the commensurability zeta function is given by (4.35). Combining the above expressions and noting that the contribution of vertices with signature $(0,0,\ell)$ and $(0,\ell,\ell)$ are the same, we see that the commensurability zeta function $Z_{\mathbf{Q}_p^3,\mathbf{Z}_p^3}(t)$ is given by

$$\begin{aligned}Z_{\mathbf{Q}_p^3}(t) = \frac{1+t^3}{1-t^3} + 2\cdot\frac{p^2+p+1}{p^2}\left(\frac{p^2t}{1-t^3}\left(\frac{1}{1-p^2t}+\frac{t}{1-p^2t^2}\right)+\frac{p^4t^3}{(1-p^2t)(1-p^2t^2)}\right)\\ +\frac{(p^2+p+1)(p+1)}{p^3}\left(\frac{t^2+t}{t^3-1}\cdot\frac{2p^4t^3}{(1-p^2t)(1-p^2t^2)}+\frac{1+t}{1-t}\cdot\frac{p^4t^2}{(1-p^2t)^2}\right)\end{aligned}$$

and after expanding the brackets, simplifying and factoring, the above expression simplifies to

$$Z_{\mathbf{Q}_p^3,\mathbf{Z}_p^3}(t)=\frac{(1+t)(1+pt)(1-pt^2)}{(1-t)(1-pt)(1-p^2t)^2}=\frac{(1-t^2)(1-pt^2)(1-p^2t^2)}{(1-t)^2(1-pt)^2(1-p^2t)^2}$$

in accordence with Theorem 4.1.5.

Chapter 5

Normal subgroup zeta function of the group $\mathbf{SL}_d^1(\mathcal{O})$

5.1 Introduction

Let G be a group. Define for every positive integer $n \in \mathbf{N}$ the number $a_n^{\trianglelefteq}(G)$ by

$$a_n^{\trianglelefteq}(G) = |\{H \trianglelefteq G \mid |G : H| = n\}|,$$

i.e. the number of normal subgroups of G of index n. In case the number $a_n^{\trianglelefteq}(G)$ is finite for every $n \in \mathbf{N}$, we define the *normal subgroup growth* of the group G by

$$s^{\trianglelefteq}(G) : \mathbf{N} \to \mathbf{N}, \quad m \mapsto s_m^{\trianglelefteq}(G) = \sum_{n=1}^{m} a_n^{\trianglelefteq}(G),$$

i.e. $s_m^{\trianglelefteq}(G)$ equals the number of normal subgroups of G of index at most m, and we define the corresponding *normal subgroup zeta function*, or in short *normal zeta function*, of G by the (formal) Dirichlet series

$$\zeta_G^{\trianglelefteq}(s) = \sum_{n=1}^{\infty} a_n^{\trianglelefteq}(G) n^{-s}, \quad s \in \mathbf{C}.$$

For a prime number p we write

$$\zeta_{G,p}^{\trianglelefteq}(s) = \sum_{n=0}^{\infty} a_{p^n}^{\trianglelefteq}(G) p^{-ns}, \quad s \in \mathbf{C},$$

for the *local factor* of $\zeta_G^{\trianglelefteq}(s)$ at p. When G is a profinite group, we should take into account the topology of G and we define $a_n^{\trianglelefteq}(G)$ to be the number of closed subgroups of G of index

n. In case G is a finitely generated profinite group, then a deep result Nikolov and Segal, see [50], says that any abstract normal subgroup of G of finite index is open. So for these groups we do not need to incorporate the condition of being closed. Groups for which the numbers $a_n^{\trianglelefteq}(G)$ are finite for all $n \in \mathbf{N}$ are, for example, finitely generated groups, because these groups have finitely many subgroups of every finite index. Many interesting groups are finitely generated. When G is a profinite group and topologically finitely generated an analogous statement holds for closed subgroups of G.

In their seminal 1998 paper [27] Grunewald, Segal and Smith introduce, among other types of zeta functions of groups, the normal subgroup zeta function. For torsion-free finitely generated nilpotent groups G they show the existence of an Euler product

$$\zeta_G^{\trianglelefteq}(s) = \prod_p \zeta_{G,p}^{\trianglelefteq}(s),$$

where the product runs over all prime numbers p, rationality of the local factors $\zeta_{G,p}^{\trianglelefteq}(s)$ and more. They are interested in what the growth of the function $s^{\trianglelefteq}(G)$ can say about the algebraic properties of the group G and vice versa. For the closely related area of subgroup growth a clear answer is given for groups of polynomial subgroup growth, which were characterised as the virtually soluble groups of finite rank in 1993 by Lubotzky, Mann and Segal [42]. This is one of the greatest achievemenst of the area of subgroup growth. For normal subgroup growth there is no such result. It is remarked in the introduction of the article [4] by Barnea and Schlage-Puchta that a slight variation of [45, Prop. 1.3.2 (ii)] yields for groups $H \leq G$ with $|G : H| < \infty$ that $s_n^{\trianglelefteq}(G) \leq s_n^{\trianglelefteq}(H) n^{|G:H|}$ for all $n \in \mathbf{N}$. And so the difficult problem remains, if a finite index subgroup of a group G can have substantially more normal subgroups than the group G itself. In contrast to subgroup growth there are simply too many groups with polynomial normal subgroup growth (including, for instance, finitely generated infinite simple groups); even if one restricts to residually finite groups, which seems reasonable, it seems daunting to extract much useful information solely from the condition of polynomial normal subgroup growth. Typically it is difficult to compute explicitly the normal zeta functions of groups, even for nicely behaved families of groups such as compact p-adic analytic groups. Very little is known about the asymptotic behaviour of $s^{\trianglelefteq}(G)$ or the properties of the zeta function $\zeta_G^{\trianglelefteq}(s)$.

In the 2001 article [44] Lubotzky shows for any finitely generated group G and every $n \in \mathbf{N}$ that $s_n^{\trianglelefteq}(G) \leq n^{c\Omega(n)}$, with $c > 0$ some constant and where $\Omega(n)$ denotes the number of prime divisors of n with multiplicity. A result of Mann [47] shows that for a non-abelian free group G we have $s_n^{\trianglelefteq}(G) > n^{c \log(n)}$ for some $c > 0$ and infinitely many $n \in \mathbf{N}$. This shows that the normal subgroup growth type of non-abelian free groups is $n^{\log(n)}$; see [4] for the definition of the *type* of a function.

For free abelian groups the corresponding normal subgroup zeta function, which coincides with the subgroup zeta function, are well-known. For an integer $d > 0$ the normal

zeta function of the free abelian group $G = \mathbf{Z}^d$ of rank d is given by

$$\zeta^{\triangleleft}_{\mathbf{Z}^d}(s) = \zeta(s)\zeta(s-1)\cdots\zeta(s-d+1),$$

with $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ the ordinary Riemann zeta function, see [12, §1] or [45, Ch. 15] for five different proofs of this identity. Using the analytic properties of $\zeta^{\triangleleft}_{\mathbf{Z}^d}(s)$ it is possible to deduce the rate of growth of $s^{\triangleleft}_N(\mathbf{Z}^d)$ as a function of N. For torsion-free finitely generated nilpotent groups G many local factors of $\zeta^{\triangleleft}_G(s)$ are computed in [27]. In [62] Voll computes the normal zeta function of torsion-free finitely generated nilpotent groups of class 2 with small centres. This applies in particular to the Heisenberg group $H(R)$, which is for a ring (commutative with 1) R defined as the subgroup

$$H(R) = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} | a, b, c \in R \right\}$$

of $\mathrm{GL}_3(R)$. Specifically we have $\zeta^{\triangleleft}_{H(\mathbf{Z})}(s) = \zeta(s)\zeta(s-1)\zeta(3s-2)$. An important step in [62] is the use of the Mal'cev correspondence, which associates to a torsion-free finitely generated nilpotent group G a $\mathbf{Q}$-Lie algebra $\mathfrak{L}(G)$. In the case where G is of nilpotency class 2, we have for every prime number p that $\zeta^{\triangleleft}_{G,p}(s) = \zeta^{\triangleleft}_{\mathfrak{L}(G),p}(s)$, with $\zeta^{\triangleleft}_{\mathfrak{L}(G),p}(s)$ enumerating the ideals of $\mathfrak{L}(G)$ of p-th power index. The local factors $\zeta^{\triangleleft}_{H(\mathcal{O}),p}(s)$ of the normal zeta function $\zeta^{\triangleleft}_{H(\mathcal{O})}(s)$, with $\mathcal{O}$ the ring of integers of a number field, have also recieved some considerable amount of attention. In [54, 55] the local factors $\zeta^{\triangleleft}_{H(\mathcal{O}),p}(s)$ have been computed for primes p which are unramified or non-split in $\mathcal{O}$; see also [22, Sect. 2] for further examples.

In general the computation of the normal zeta function of a group G is hard. However, sometimes we understand the structure of the group G well enough that we are able to compute the normal zeta function explicitly. In Chapter 5 we focus on a particular family of groups for which we can say something concrete about the normal zeta function and in some cases calculate the normal zeta function explicitly.

For the remainder of the introduction let K be a non-Archimedean local field, write $\mathcal{O}$ for the ring of integers of K, let $\mathfrak{p}$ be the unique maximal ideal of $\mathcal{O}$ and let $k = \mathcal{O}/\mathfrak{p}$ be the finite residue field of characteristic $\mathrm{char}\, k = p$. These local fields play a central role in algebraic number theory; typical examples are the field $\mathbf{Q}_p$ of p-adic numbers and the field $\mathbf{F}_p(\!(T)\!)$ of Laurent series over a finite field $\mathbf{F}_p$. Let $d > 1$ be an integer and consider the group $G_0 = \mathrm{SL}_d(\mathcal{O})$. For a positive integer $n \in \mathbf{N}$ the *n-th principal congruence subgroup* $G_n = \mathrm{SL}^n_d(\mathcal{O})$ of the group $G_0 = \mathrm{SL}_d(\mathcal{O})$ is defined by

$$\mathrm{SL}^n_d(\mathcal{O}) = \ker(\mathrm{SL}_d(\mathcal{O}) \to \mathrm{SL}_d(\mathcal{O}/\mathfrak{p}^n)),$$

here we consider the reduction of the matrix entries modulo $\mathfrak{p}^n$. The groups $\mathrm{SL}^n_d(\mathcal{O})$ are examples of pro-p groups.

In case K is the field $\mathbf{Q}_p$ of p-adic rational numbers or the field $\mathbf{F}_p(\!(T)\!)$ of Laurent series in T with coefficients in the finite field $\mathbf{F}_p$, the (normal) subgroup zeta functions of the groups $\mathrm{SL}_d^1(\mathcal{O})$ have been studied. In [45, Sect. 4.3] bounds for the subgroup growth of the groups $\mathrm{SL}_d^1(\mathcal{O})$ with $\mathcal{O} = \mathbf{F}_p[\![T]\!]$ are obtained. In some cases the normal subgroup zeta functions of the groups $\mathrm{SL}_d^1(\mathcal{O})$ have also been studied. In [58] Snopce computes the normal zeta function for the group $\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])$ for all prime numbers $p > 2$, showing that

$$\zeta^{\trianglelefteq}_{\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])}(s) = \frac{1 + (p^2+p+1)(t+t^2+pt^3)}{1-t^3}, \quad t = p^{-s},$$

from which it follows for an integer $m \in \mathbf{N}$ that

$$a^{\trianglelefteq}_{p^m}(\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])) = \begin{cases} p^2+p+1 & \text{if } 3 \nmid m \\ p^3+p^2+p+1 & \text{if } 3 \mid m. \end{cases}$$

For a fixed prime number $p > 2$ Snopce also shows that the group $\mathrm{SL}_2^1(\mathbf{F}_p[\![T]\!])$ has the same normal zeta function as the group $\mathcal{Q}(s,r)$, defined by Ershov in [24]. In [21, Cor. 4.10] du Sautoy provides a formula for the normal zeta function of the groups $\mathrm{SL}_2^n(\mathbf{Z}_p)$ for $n \in \mathbf{N}$ and $p > 2$ a prime number. In Theorem 5.1.5 we compute the normal zeta function of $\mathrm{SL}_2^1(\mathbf{Z}_p)$ for prime numbers $p > 2$, which is different from the one presented in [21, Cor. 4.10]. We believe our formula is correct. We are supported in this by the paper [3] by Barnea and Guralnick, they prove in [3, Thm. 1.3] that the sequence $(a_n^{\trianglelefteq}(\mathrm{SL}_2^1(\mathbf{Z}_p)))_{n\geq 1}$ is eventually periodic. Whereas the formula in [21, Cor. 4.10] suggests that $a_n^{\trianglelefteq}(\mathrm{SL}_2^1(\mathbf{Z}_p))$ grows polynomially with n. It was pointed out by Klopsch in [36, p. 57], that there is a mistake in [21, Lem. 4.6]. This could possibly explain the different formula in [21, Cor. 4.10]. It is also worth mentioning that [3, Thm. 1.4] proves that $a_n^{\trianglelefteq}(\mathrm{SL}_d^1(\mathbf{F}_p[\![T]\!]))$ is not bounded as a function of n in case $p \mid d$ in contrast to the case $p \nmid d$, where it is bounded.

Our investigation into the normal zeta function of the groups $\mathrm{SL}_d^1(\mathcal{O})$ is motivated by a yet to be published paper titled *Normal subgroups of Chevalley groups* by Klopsch and Snopce [37]; generalising earlier work of Barnea, Guralnick and Snopce [3, 58]. They set out to prove the following. Let $\mathfrak{g}$ be a Chevalley Lie algebra over a field F, associated to a root system of Chevalley type X. Suppose that char $F \neq 2$, if X is one of A_*, B_*, C_*, D_*, F_4, and that char $F \neq 3$, if X is G_2. Let z be a non-central element of $\mathfrak{g}$, then $[\mathfrak{g}, [\mathfrak{g}, [\mathfrak{g}, x]]]$ equals $\mathfrak{g}$. In Theorem 5.1.1 we strengthen their result for the simple Lie algebras of Chevalley type A_*. The finiteness result discovered and proved by Klopsch and Snopce is very surprising. Besides its fundamental nature it has very tangible applications, as noted by Klopsch and Snopce. For instance, their result places severe restrictions on the normal subgroup structure and describe properties of the normal subgroup zeta functions of the groups $\mathrm{SL}_d^1(\mathcal{O})$ of increasing rank. In small cases, one should be able to compute the corresponding normal zeta functions explicitly. This is also what we do in Chapter 5.

Before we state our results, we first discuss our method of computation which is similar to the approach taken in [58] by Snopce. Let $d > 1$ be an integer and let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ satisfying $p = \mathrm{char}\ k \nmid 2d$. The first step of

our computation is to translate our problem of counting normal subgroups of $G = \mathrm{SL}_d^1(\mathcal{O})$ to counting Lie ideals in a suitably chosen graded Lie algebra; for more on this construction see [43]. The subgroups $G_n = \mathrm{SL}_d^n(\mathcal{O})$ of G are the principal congruence subgroups, they satisfy $\bigcap_{n=1}^{\infty} G_n = \{1\}$, $(G_m, G_n) \leq G_{m+n}$ and $G_n^p \leq G_{n+1}$ for all $m, n \in \mathbf{N}$. We associate to the group G the graded Lie algebra over $\mathbf{F}_p$ given by

$$L(G) = \bigoplus_{n=1}^{\infty} G_n/G_{n+1}.$$

For more on this Lie algebra, its bracket and its grading, see Section 5.2 and Section 5.3. To a closed normal subgroup $N \trianglelefteqslant G$ we associate the Lie ideal $L(N)$ of $L(G)$ defined by

$$L(N) = \bigoplus_{n=1}^{\infty} (N \cap G_n)G_{n+1}/G_{n+1}.$$

The question arises how the Lie ideals of $L(G)$ look like and which Lie ideals of $L(G)$ are of the form $L(N)$ for some closed normal subgroup N of G. This is answered in Proposition 5.3.12.

Write $\mathfrak{sl}_d(k)$ for the special linear Lie algebra of Chevalley type A_{d-1} over the field k with the usual bracket $[x, y] = xy - yx$ for $x, y \in \mathfrak{sl}_d(k)$; see Section 5.4.1. For a subspace $V \subseteq \mathfrak{sl}_d(k)$ we write $[\mathfrak{sl}_d(k), V]$ for the subspace of $\mathfrak{sl}_d(k)$ spanned by all the commutators $[x, y]$ with $x \in \mathfrak{sl}_d(k)$ and $y \in V$. We prove in Lemma 5.3.1 that there is an isomorphism $G_n/G_{n+1} \cong \mathfrak{sl}_d(k)$ of abelian groups for all $n \in \mathbf{N}$. This results in an isomorphism

$$\varphi : L(G) \to t \cdot \mathfrak{sl}_d(k)[t]$$

of graded Lie algebras over $\mathbf{F}_p$ (see 5.3), here $t \cdot \mathfrak{sl}_d(k)[t]$ consists of the polynomials in t with coefficients from the Lie algebra $\mathfrak{sl}_d(k)$ and constant coefficient equal to zero. Understanding how Lie ideals of $L(G)$ look like is crucial for computing the normal zeta function of G. Our next theorem, see also Theorem 5.6.5, extends earlier unpublished results for simple Lie algebras of Chevalley type A_*, as discussed in [37].

Theorem 5.1.1. *Let $d > 1$ be an integer and let k be a field with* $\mathrm{char}\ k \nmid 2d$. *For all non-zero $x \in \mathfrak{sl}_d(k)$ we have*

$$[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), x]] = \mathfrak{sl}_d(k).$$

Actually, a slightly stronger result is proven in Theorem 5.6.5 in Section 5.6.1, however the above theorem is all we need for our discussion. A consequence of the above theorem is Proposition 5.3.7. It states that any closed normal subgroup $\{1\} \neq N \trianglelefteqslant G$ satisfies

$$G_{n+2} < N \leq G_n, \quad N \not\subseteq G_{n+1}$$

for some unique $n \in \mathbf{N}$. In particular G is just infinite, i.e. every closed non-trivial closed normal subgroup of G has finite index (and hence is also open). Consequently every Lie ideal $L(N)$ in $L(G) \cong t \cdot \mathfrak{sl}_d(k)[t]$ is of the form

$$Vt^n \oplus Wt^{n+1} \oplus t^{n+2}\mathfrak{sl}_d(k)[t] \tag{5.1}$$

for some non-zero $\mathbf{F}_p$-subspaces $V, W \subseteq \mathfrak{sl}_d(k)$. Necessary and sufficient conditions for (5.1) to be an ideal of $L(G)$ are that the spaces V, W satisfy

$$[\mathfrak{sl}_d(k), V] \subseteq W.$$

Define the number $\delta_K \in \{0, 1\}$ by

$$\delta_K = \begin{cases} 1 & \text{when } K \text{ is an unramified extension of } \mathbf{Q}_p; \\ 0 & \text{otherwise.} \end{cases}$$

The Lie ideals $L(N)$ coming from a closed normal subgroup $\{1\} \neq N \trianglelefteqslant G$ are of the form as in (5.1) subject to the condition

$$\delta_K V + [\mathfrak{sl}_d(k), V] \subseteq W, \tag{5.2}$$

see also Proposition 5.3.12. The case distinction for K comes from the p-th power map on G, it enforces an extra condition on Lie ideals coming from closed normal subgroups of G; see also Lemma 5.3.10 and Proposition 5.3.12. We will encounter this when computing the normal zeta function of $\mathrm{SL}_d^1(\mathbf{Z}_p)$. We show that there are $|\mathfrak{sl}_d(k) : W|^{\dim_{\mathbf{F}_p} V}$ closed normal subgroups of G, whose corresponding ideal in $t \cdot \mathfrak{sl}_d(k)[t]$ is given by (5.1) subject to the condition in (5.2).

The above discussion leads to the next theorem, which presents a general formula for the normal zeta function of the groups $\mathrm{SL}_d^1(\mathcal{O})$; see Theorem 5.3.14.

Theorem 5.1.2 (Klopsch, Snopce, T.)**.** *Let $d > 1$ be an integer and let p be a prime number with $p \nmid 2d$. Let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and residue class field k. Write $L = \mathfrak{sl}_d(k)$. The normal zeta function $\zeta_G^{\trianglelefteqslant}(s)$ for the group $G = \mathrm{SL}_d^1(\mathcal{O})$ is given by*

$$\zeta_G^{\trianglelefteqslant}(s) = \frac{1}{1 - |L|^{-s}} \sum_{0 \neq V \subseteq L} |L : V|^{-s} \left(\sum_{\delta_K V + [V,L] \subseteq W \subseteq L} |L : W|^{-s + \dim_{\mathbf{F}_p} V} \right),$$

where V, W are $\mathbf{F}_p$-subspaces of L.

The above expression shows that the normal zeta function of $\mathrm{SL}_d^1(\mathcal{O})$ is a rational function in p^{-s} and we recover the fact that the sequence $(a_n^{\trianglelefteqslant}(\mathrm{SL}_d^1(\mathcal{O})))_{n \geq 1}$ is eventually periodic; this generalises the result in [3, Thm. 1.3]. The formula for the normal zeta function depends on the residue field k, but except for the occurrence of δ_K, it does not depend on the ramification behaviour of the maximal ideal $\mathfrak{p}$. We list two important corollaries.

Corollary 5.1.3 (Klopsch, Snopce, T.). *Let $d > 1$ be an integer, let p be a prime number with $p \nmid 2d$ and write $f = [k : \mathbf{F}_p]$ for the degree of the field extension $k/\mathbf{F}_p$. Then there exists a polynomial $Q(X, Y) \in \mathbf{Z}[X, Y]$ with $\deg_Y Q = 2(d^2 - d)f - 1$ such that*

$$\zeta^{\triangleleft}_{\mathrm{SL}^1_d(\mathcal{O})}(s) = \frac{Q(p, p^{-s})}{1 - (p^{-s})^{(d^2-1)f}}.$$

Corollary 5.1.4. *Let $d > 1$ be an integer and let p be a prime number with $p \nmid 2d$. Let $K/\mathbf{Q}_p$ be an unramified extension with $\mathcal{O}$ the ring of integers of K and write $f = [k : \mathbf{F}_p]$ for the degree of the field extension $k/\mathbf{F}_p$. Then the groups $\mathrm{SL}^1_d(\mathcal{O})$ and $\mathrm{SL}^1_d(\mathbf{F}_{p^f}[\![T]\!])$ have the same normal subgroup zeta function.*

Hence the groups $\mathrm{SL}^1_d(\mathcal{O})$ and $\mathrm{SL}^1_d(\mathbf{F}_{p^f}[\![T]\!])$ in the corollary are two examples of *normally isospectral* groups.

In order to compute the normal zeta function of the groups $\mathrm{SL}^1_d(\mathcal{O})$ explicitly, we need to understand the behaviour of the map

$$V \mapsto \delta_K V + [\mathfrak{sl}_d(k), V]$$

where V is a subspace of $\mathfrak{sl}_d(k)$. We need to know for all integers $1 \leq m, n \leq d^2 - 1$ how many subspaces V of $\mathfrak{sl}_d(k)$ there are satisfying

$$\dim_{\mathbf{F}_p} V = m \quad \text{and} \quad \dim_k(\delta_K V + [\mathfrak{sl}_d(k), V]) = n.$$

These computations are done in Section 5.4 from which we derive the normal zeta function of the groups $\mathrm{SL}^1_2(\mathbf{Z}_p)$ ($p > 2$), $\mathrm{SL}^1_3(\mathbf{F}_p[\![T]\!])$ and $\mathrm{SL}^1_3(\mathbf{Z}_p)$ ($p > 3$). We also recover the normal zeta function for the group $\mathrm{SL}^1_2(\mathbf{F}_p[\![T]\!])$ as in [58].

Theorem 5.1.5. *Let $p > 2$ be a prime number. The normal zeta function of the group $\mathrm{SL}^1_2(\mathbf{Z}_p)$ is given by*

$$\zeta^{\triangleleft}_{\mathrm{SL}^1_2(\mathbf{Z}_p)}(s) = 1 + \frac{(p^2 + p + 1)t}{1 - t}, \quad t = p^{-s}$$

and hence for any $m \in \mathbf{N}$ we have $a^{\triangleleft}_{p^m}(\mathrm{SL}^1_2(\mathbf{Z}_p)) = p^2 + p + 1$.

Consequently, the normal subgroup growth of the group $\mathrm{SL}^1_2(\mathbf{Z}_p)$ for $p > 2$ is given by

$$s^{\triangleleft}_{p^n}(\mathrm{SL}^1_2(\mathbf{Z}_p)) = 1 + n(p^2 + p + 1), \quad n \in \mathbf{N}.$$

Theorem 5.1.6. *Let $p > 3$ be a prime number. The normal zeta functions of the groups $\Gamma_0 = \mathrm{SL}^1_3(\mathbf{F}_p[\![T]\!])$ and $\Gamma_1 = \mathrm{SL}^1_3(\mathbf{Z}_p)$ are of the form*

$$\zeta^{\triangleleft}_{\Gamma_\ell}(s) = \frac{1 + a^\ell_1(p)t + \ldots + a^\ell_{11}(p)t^{11}}{1 - t^8}$$

where $t = p^{-s}$, $\ell \in \{0,1\}$ *and* $a_i^\ell(X) \in \mathbf{Z}[X]$ *are polynomials in* X *with non-negative coefficients. Write* $\mathbf{a}_\ell = (\deg a_1^\ell(X), \ldots, \deg a_{11}^\ell(X))$ *for the list of degrees of the polynomials* $a_1^\ell, \ldots, a_{11}^\ell$. *We then have*

$$\mathbf{a}_0 = (7, 12, 15, 16, 15, 12, 10, 10, 10, 10, 8)$$

and

$$\mathbf{a}_1 = (7, 12, 15, 16, 15, 12, 9, 8, 9, 9, 7).$$

The explicit polynomials a_i^ℓ can be found in Section 5.6.7. The difference between the two sequences $\mathbf{a}_0, \mathbf{a}_1$ is explained by the fact that the condition $V + [L, V] \subseteq W$ is more restrictive than the condition $[L, V] \subseteq W$.

It would be interesting to know the explicit normal zeta functions of the groups $\mathrm{SL}_2^1(\mathcal{O})$ and $\mathrm{SL}_3^1(\mathcal{O})$ with $\mathcal{O}$ the ring of integers of a non-Archimedean field K which is a finite extension of $\mathbf{Q}_p$ or $\mathbf{F}_p(\!(T)\!)$. We can use the formula in Theorem 5.1.2 to do this. The calculations for the Lie algebra $\mathfrak{sl}_3(k)$ in Section 5.4 are quite extensive and elaborate. It would be interesting to know, if the same can be done for the Lie algebra $\mathfrak{sl}_4(k)$ to compute the normal zeta functions of $\mathrm{SL}_4^1(\mathbf{Z}_p)$ and $\mathrm{SL}_4^1(\mathbf{F}_p[\![T]\!])$. The calculations in $\mathfrak{sl}_3(k)$ involve a careful analysis of the interaction between elements with different Jordan normal form. Because there are more different Jordan normal forms of elements of $\mathfrak{sl}_4(k)$, we expect that the calculations for $\mathfrak{sl}_4(k)$ will be significantly harder. Perhaps writing down explicit polynomials is not the best way to approach the calculations for $\mathfrak{sl}_d(k)$ with $d \geq 4$. An alternative could be to try to find a description for the coefficients in the numerator of $\zeta^{\trianglelefteq}_{\mathrm{SL}_4^1(\mathcal{O})}(s)$ in terms of varieties over k.

In a different direction it would be interesting to see, if we can compute the normal zeta function of groups like $\mathrm{Sp}_4^1(\mathbf{Z}_p)$ or $\mathrm{Sp}_4^1(\mathbf{F}_p[\![T]\!])$ by making use of the result of Klopsch and Snopce for the Lie algebra $\mathfrak{sp}_4(k)$. A first step could be to investigate, if one can improve on their result by showing that $[\mathfrak{sp}_4(k), [\mathfrak{sp}_4(k), x]] = \mathfrak{sp}_4(k)$ holds for all non-zero $x \in \mathfrak{sp}_4(k)$, with a possible restriction on the characteristic of k.

5.2 Lie ring of a group

In this section we introduce methods from Lie theory to study certain questions about groups. The idea of using Lie theory to study groups was first introduced by Magnus in [48], one of the applications he proposed was to use it to study the restricted Burnside problem. We introduce the Lie ring associated to a group and list some properties of it. For more details see [60].

Let G be a group and let

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

be a descending chain of subgroups of G satisfying

$$\bigcap_{i=1}^{\infty} G_i = \{1\}$$

and

$$(G_i, G_j) \subseteq G_{i+j} \tag{5.3}$$

for all $i, j \in \mathbf{N}$. Following [58] we call the collection $(G_i)_{i\geq 1}$ of groups a *filtration of* G. A direct consequence of the condition (5.3) is that for all integers $i \in \mathbf{N}$ we have $G_i \trianglelefteq G$, i.e. G_i is a normal subgroup of G. Moreover, for all integers $i \in \mathbf{N}$ we have the inclusions $(G_i, G_i) \subseteq G_{2i} \subseteq G_{i+1}$ and hence the quotient G_i/G_{i+1} is abelian. We associate to G the abelian group

$$L(G) = \bigoplus_{i=1}^{\infty} G_i/G_{i+1}.$$

The rules for adding and taking inverses in G_i/G_{i+1}, which extend linearly to $L(G)$, are

$$xG_{i+1} + yG_{i+1} = xyG_{i+1} \quad \text{and} \quad x^{-1}G_{i+1} = -(xG_{i+1})$$

for $x, y \in G_i$. The assumption on the groups G_i in (5.3) can be used to turn the abelian group $L(G)$ into a *graded Lie ring*. For this we define a bracket $[-,-]$ on homogeneous elements by

$$[xG_{i+1}, yG_{j+1}] = (x, y)G_{i+j+1} \in G_{i+j}/G_{i+j+1},$$

where $x \in G_i$, $y \in G_j$ and $i, j \in \mathbf{N}$, and extend linearly to all of $L(G)$. Here the commutator of $x, y \in G$ is defined as $(x, y) = x^{-1}y^{-1}xy$.

The more we know of the group G and its subgroups G_i, the more we can say about the Lie ring $L(G)$. One particularly important assumption on the group G is the following. Let p be a prime number and assume that

$$G_i^p \leq G_{i+1} \tag{5.4}$$

for all $i \in \mathbf{N}$. Here G_i^p stands for the subgroup of G_i generated by all the p-th powers of elements of G_i (if G is profinite, then we consider the closed subgroup generated by the p-th powers). The assumption in (5.4) for all $i \in \mathbf{N}$ implies that every element of G_i/G_{i+1} has additive order dividing p. Therefore $L(G)$ is a vector space over $\mathbf{F}_p$ and hence we may consider $L(G)$ as a *graded Lie algebra over* $\mathbf{F}_p$.

To a subgroup $H \leq G$ (if G is profinite, we assume H to be closed) we associate $L(H)$, a graded Lie subalgebra over $\mathbf{F}_p$ of $L(G)$, defined by

$$L(H) = \bigoplus_{i=1}^{\infty} (H \cap G_i) G_{i+1}/G_{i+1}.$$

Some properties of H can be deduced from the Lie subalgebra $L(H)$. For example, if we have $G_n \leq H$ for some integer $n \in \mathbf{N}$, then we have the identity

$$|G : H| = |L(G) : L(H)|, \tag{5.5}$$

relating the index of the two groups to the index of the corresponding Lie algebras. Moreover, when $H \trianglelefteq G$ is a normal subgroup of G, then one can show that $L(H)$ is a Lie ideal of $L(G)$, meaning that

$$[L(H), L(G)] \subseteq L(H).$$

Finally, let G be a profinite group with a filtration $(G_n)_{n \geq 1}$ of closed subgroups of G. For a closed subgroup $H \leq G$ and $n \in \mathbf{N}$ we have the equivalence

$$G_n \leq H \quad \Leftrightarrow \quad L(G_n) \subseteq L(H). \tag{5.6}$$

5.3 On the Lie algebra $L(G)$ of $G = \mathbf{SL}_d^1(\mathcal{O})$

5.3.1 Determination of $L(G)$

Let $d > 1$ be an integer and let K be a non-Archimedean local field with ring of integers $\mathcal{O}$. Write $\mathfrak{p}$ for the unique maximal ideal of $\mathcal{O}$ with π some uniformiser of $\mathfrak{p}$ and let p be the characteristic of the residue field $k = \mathcal{O}/\mathfrak{p}$. In this section we determine the Lie algebra $L(G)$ for the first principle congruence subgroup $G = \mathrm{SL}_d^1(\mathcal{O})$ of $\mathrm{SL}_d(\mathcal{O})$. Recall that the principle congruence subgroups of $\mathrm{SL}_d(\mathcal{O})$ are defined by

$$G_n = \ker\left(\mathrm{SL}_d(\mathcal{O}) \to \mathrm{SL}_d(\mathcal{O}/\mathfrak{p}^n)\right), \quad n \in \mathbf{N},$$

for more details see Chapter 2. One can show that the principle congruence subgroups $(G_n)_{n \geq 1}$ form a filtration of G. In fact, this filtration coincides with the lower central series of G if $p > 2$. It is a consequence of Lemma 5.3.1 that these subgroups G_n satisfy $G_n^p \leq G_{n+1}$ for all $n \in \mathbf{N}$. Assuming this, we have for the group G the corresponding graded Lie algebra $L(G)$ over $\mathbf{F}_p$ (see Section 5.2), given by

$$L(G) = \bigoplus_{n=1}^{\infty} G_n/G_{n+1}. \tag{5.7}$$

Recall that $\mathfrak{sl}_d(k)$ is the special linear Lie algebra over k of Chevalley type A_{d-1}. To simplify the notation we often use the abbreviation $L = \mathfrak{sl}_d(k)$, when d and k are understood to be known. In Lemma 5.3.1 we show that there is an isomorphism of (abelian) groups $G_n/G_{n+1} \cong \mathfrak{sl}_d(k)$ for all integers $n \in \mathbf{N}$. Combining these isomorphisms for every summand of $L(G)$, we get an isomorphism

$$\varphi : L(G) \to t \cdot L[t] \tag{5.8}$$

of $\mathbf{F}_p$-vector spaces; here $t \cdot L[t]$ consists of polynomials in the variable t with coefficients from L and with zero constant term. The restriction of φ to G_n/G_{n+1} induces an isomorphism

$$G_n/G_{n+1} \cong Lt^n. \tag{5.9}$$

To be more precise, let $x \in G_n$ be an element and write $x = I + X\pi^n$ with $X \in \mathrm{Mat}_d(\mathcal{O})$ some matrix, then

$$\varphi(xG_{n+1}) = Xt^n,$$

where X is to be read modulo $\mathfrak{p}$. For more details see Lemma 5.3.1. The reason we introduced the variable t is that in this way φ is also an isomorphism of (graded) Lie algebras. The bracket on $t \cdot L[t]$ that makes it into a Lie algebra is, for integers $i, j \in \mathbf{N}$ and elements $a, b \in L$, given by $[at^i, bt^j] = [a, b]t^{i+j}$, with $[a, b] = ab - ba$ the ordinary bracket on L, and extended linearly to the whole of $t \cdot L[t]$. For integers $i, j \in \mathbf{N}$ and elements $x \in G_i, y \in G_j$ we have

$$[\varphi(xG_{i+1}), \varphi(yG_{j+1})] = \varphi([xG_{i+1}, yG_{j+1}]).$$

Hence φ is actually an isomorphism of Lie algebras. For the Lie-ideal $L(G_n)$ we get through φ an isomorphism

$$L(G_n) \cong t^n L[t].$$

The next lemma is well-known, it determines the quotients G_n/G_{n+1} for $n \in \mathbf{N}$.

Lemma 5.3.1. *Let $n \in \mathbf{N}$ be a positive integer and let G_n, G_{n+1} be as above, then we have an isomorphism of abelian groups*

$$G_n/G_{n+1} \cong \mathfrak{sl}_d(k).$$

Proof. Let $X \in \mathrm{Mat}_d(\mathcal{O})$ be a matrix such that $I + X\pi^n \in G_n$. By expanding $\det(I + X\pi^n)$ as a polynomial in the entries of X we get

$$1 \equiv \det(I + X\pi^n) \equiv 1 + \mathrm{Tr}(X)\pi^n \mod \mathfrak{p}^{n+1}$$

and hence $\mathrm{Tr}(X) \equiv 0 \mod \mathfrak{p}$. Define the map

$$\varphi : G_n \to \mathfrak{sl}_d(k), I + X\pi^n \mapsto X \mod \mathfrak{p}$$

with $X \in \mathrm{Mat}_d(\mathcal{O})$. One verifies that φ is a group homomorphism with kernel

$$\ker \varphi = \{I + X\pi^n \in G_n \mid X \equiv 0 \mod \mathfrak{p}\} = G_{n+1}.$$

For $1 \leq i < j \leq d$ and $\lambda \in k$ we have $I + \lambda E_{ij}\pi^n, I + \lambda E_{ji}\pi^n \in G_n$ and for $1 \leq i \leq d-1$ we have $I + \lambda(E_{ii} - E_{i+1,i+1} + E_{i,i+1} - E_{i+1,i})\pi^n \in G_n$. For every $\lambda \in k$ the image of φ contains therefore the off-diagonal elements $\lambda E_{ij}, \lambda E_{ji}$, $1 \leq i < j \leq n$ and the diagonal elements $\lambda(E_{ii} - E_{i+1,i+1})$, $1 \leq i \leq n-1$. Together these elements generate $\mathfrak{sl}_d(k)$ and hence φ is surjective. □

Remark 5.3.2. Because the characteristic of k is p, it follows from the above lemma that for all $x \in G_n$ we have $\varphi(x^p G_{n+1}) = p\varphi(xG_{n+1}) = 0$ and hence that $G_n^p \leq G_{n+1}$ for all $n \in \mathbf{N}$.

The next lemma deals with the groups G_n^p for integers $n \in \mathbf{N}$. Depending on the field K we can significantly improve on the result $G_n^p \leq G_{n+1}$.

Lemma 5.3.3. *Let $n \in \mathbf{N}$ be a positive integer and let K, p and G_n, G_{n+1} be as above. We assume $p > 2$. If* char $K = p$, *then we have $G_n^p \leq G_{pn}$. If* char $K = 0$ *and K is* not *an unramified extension of $\mathbf{Q}_p$, then we have $G_n^p \leq G_{n+2}$. If* char $K = 0$ *and K is an unramified extension of $\mathbf{Q}_p$, then we have $G_n^p \leq G_{n+1}$.*

Proof. It follows from Lemma 5.3.1 that in any case we have $G_n^p \leq G_{n+1}$. Let $x \in G_n$ be an element and write $x = I + X\pi^n$ for some matrix $X \in \mathrm{Mat}_d(\mathcal{O})$. Suppose that char $K = p$, then we have

$$x^p = I + X^p \pi^{pn}.$$

Since $v(X^p\pi^{pn}) \geq pn$ we see that $x^p \in G_{pn}$; see Chapter 2 for the definition of the extension of the valuation to $\mathrm{Mat}_d(K)$. Next, suppose that K is a finite extension of $\mathbf{Q}_p$ with ramification index $e > 1$, then we have by expanding the product

$$x^p = I + \sum_{\ell=1}^{p-1} \binom{p}{\ell} X^\ell \pi^{\ell n} + X^p \pi^{pn}.$$

For $1 \leq \ell \leq p-1$ we have $p \mid \binom{p}{\ell}$, so $v(\binom{p}{\ell} X^\ell \pi^{\ell n}) \geq e + \ell n$ and $v(X^p\pi^{pn}) \geq pn$. Using that $p > 2$ and $e > 1$, we see that $e + \ell n \geq n + 2$ and $pn \geq n + 2$, showing that $x^p \in G_{n+2}$. □

When K has characteristic p, we have $G_n^p \leq G_{pn}$ for any $n \in \mathbf{N}$. This is connected to the notion of restricted Lie algebras. We already know by Lemma 5.3.1 that the groups G_n/G_{n+1} and G_{n+1}/G_{n+2} are isomorphic for every integer $n \in \mathbf{N}$. In the case of an unramified extension of $\mathbf{Q}_p$ the next lemma shows, that the p-th power map on G induces an isomorphism between G_n/G_{n+1} and G_{n+1}/G_{n+2}.

Lemma 5.3.4. *Let $n \in \mathbf{N}$ be a positive integer, let $p > 2$ be a prime number, let K be an unramified extension of $\mathbf{Q}_p$ and let $\varphi, G_n, G_{n+1}, G_{n+2}$ be as above. The map*

$$\psi_n : G_n/G_{n+1} \to G_{n+1}/G_{n+2}, \quad xG_{n+1} \mapsto x^p G_{n+2}$$

is an isomorphism of $\mathbf{F}_p$-vector spaces. Under the isomorphism $\varphi : L(G) \to t \cdot L[t]$ the map ψ_n induces the multiplication by t map between Lt^n and Lt^{n+1}.

Proof. Because K is an unramified extension of $\mathbf{Q}_p$ we take $\pi = p$ as the uniformiser for $\mathfrak{p}$. For the rest of the proof we let $x, y \in G_n$ be two elements and write $x = I + Xp^n, y = I + Yp^n$ for some $X, Y \in \mathrm{Mat}_d(\mathcal{O})$. Note that the inverse of x in G_n is given by

$$x^{-1} = I - Xp^n + X^2p^{2n} - X^3p^{3n} + \dots.$$

Suppose $xG_{n+1} = yG_{n+1}$, then $xy^{-1} \in G_{n+1}$. We have

$$xy^{-1} \equiv (I + Xp^n)(I - Yp^n) \equiv I + (X - Y)p^n \mod \mathfrak{p}^{n+1}$$

and so we see that $X \equiv Y \mod \mathfrak{p}$. Using that $x^p \equiv I + Xp^{n+1} \mod \mathfrak{p}^{n+2}$, we compute along similar lines

$$x^p y^{-p} \equiv (I + Xp^{n+1})(I - Yp^{n+1}) \equiv I + (X - Y)p^{n+1} \equiv I \mod \mathfrak{p}^{n+2}.$$

It follows that $x^p y^{-p} \in G_{n+2}$ and hence $x^p G_{n+2} = y^p G_{n+2}$. The above argument can be reversed to show that $x^p G_{n+2} = y^p G_{n+2}$ implies that $xG_{n+1} = yG_{n+1}$, i.e. that ψ_n is injective. Together with $|G_n : G_{n+1}| = |G_{n+1} : G_{n+2}|$ this shows that ψ_n is a bijection. An approach similar to the above shows that

$$y^{-p}x^{-p}(xy)^p \equiv I \mod \mathfrak{p}^{n+2},$$

which is equivalent to

$$\psi_n(xG_{n+2} + yG_{n+2}) = \psi_n(xG_{n+1}) + \psi_n(yG_{n+1}).$$

This shows that ψ_n is an isomorphism of $\mathbf{F}_p$-vector spaces. For $x \in G_n$ we compute

$$\varphi(\psi_n(xG_{n+1})) = \varphi(x^p G_{n+2}) = \varphi(xG_n) \cdot t,$$

under the isomorphism $\varphi : L(G) \to t \cdot L[t]$ the map ψ_n therefore induces the multiplication by t map between Lt^n and Lt^{n+1}. □

5.3.2 Formula for normal zeta function

In this section we establish the general formula for the normal zeta function of $G = \mathrm{SL}_d^1(\mathcal{O})$. For a closed normal subgroup $H \trianglelefteqslant G$ we first investigate how its corresponding Lie ideal $L(H)$ of $L(G)$ looks like. Secondly, we compute, for a fixed Lie ideal of $L(G)$, the number of closed normal subgroups of G, which have this fixed Lie ideal as their corresponding Lie ideal in $L(G)$. We continue to use the same notation as in the previous section.

The next theorem is solely about the Lie algebra $L = \mathfrak{sl}_d(k)$. We give a proof of this theorem in Section 5.6.1, where we actually prove a slightly stronger result; see Theorem 5.6.5. This theorem was inspired by an upcoming paper by Klopsch and Snopce [37], in which they prove a similar result for Chevalley Lie algebras. Theorem 5.3.5 is a strengthening of their result for the case of a Lie algebra of Chevalley type A_{d-1}. This theorem is crucial for the computation of the normal zeta function of the group $G = \mathrm{SL}_d^1(\mathcal{O})$, as it allows us to prove Proposition 5.3.7.

Theorem 5.3.5. *Let $d > 1$ be an integer. Let k be any field satisfying* $\mathrm{char}\, k \nmid 2d$ *and write $L = \mathfrak{sl}_d(k)$ for the special linear Lie algebra of Chevalley type A_{d-1}. For any $0 \neq x \in L$ we have*

$$[[x, L], L] = L.$$

Remark 5.3.6. The assumption that $\mathrm{char}\, k \nmid 2d$ is necessary for the statement of the above theorem to hold. For instance, if $\mathrm{char}\, k \mid d$, take x to be the identity matrix I (note $\mathrm{Tr}(I) = d = 0$, so $I \in \mathfrak{sl}_d(k)$), then we see $[I, L] = 0$. In case $\mathrm{char}\, k = 2$ there exist non-zero elements $x \in L$ for which $[[x, L], L] \neq L$; see Theorem 5.6.5.

The next proposition shows that every closed normal subgroup of G is sandwiched between two principal congruence subgroups G_n, G_{n+2} for some $n \in \mathbf{N}$. The statement and the proof of this proposition already appear in [58] as Lemma 3.2 for the case $d = 2$. With Theorem 5.3.5 we can generalise it to arbitrary $d > 1$. The proof is slighlty rewritten to fit the notation of this chapter.

Proposition 5.3.7. *Let $d > 1$ be an integer, let K be a local field with ring of integers $\mathcal{O}$ and assume that the residue field k of K satisfies* $\mathrm{char}\, k \nmid 2d$. *Write $G = \mathrm{SL}_d^1(\mathcal{O})$ and let $\{1\} \neq H \trianglelefteqslant G$ be a closed normal subgroup. Then there exists a unique positive integer $n \in \mathbf{N}$ such that the following two conditions hold:*

$$G_{n+2} < H \leq G_n, \quad H \nsubseteq G_{n+1}.$$

Proof. Because $H \neq \{1\}$ there exists a largest integer $n \in \mathbf{N}$ such that $H \leq G_n$ and hence there exists $h \in H$ with $h \notin G_{n+1}$. Write $\varphi(L(H)) = \bigoplus_{i=1}^{\infty} L_i t^i$, so the L_i are $\mathbf{F}_p$-subspaces of L. Let $u \in L_n$ be such that $ut^n = \varphi(hG_{n+1})$, since $h \notin G_{n+1}$ we have $u \neq 0$. Set

$U = [u, L]$, then by Theorem 5.3.5 we have $[U, L] = L$. Because H is normal in G, $L(H)$ is an ideal of $L(G)$ and hence $[L(H), L(G)] \subseteq L(H)$. This implies that for all $\in \mathbf{N}$ we have

$$Ut^{m+n} = [ut^n, Lt^m] \subseteq L_{m+n}t^{m+n},$$

so $U \subseteq L_{m+n}$ and similarly

$$Lt^{m+n+1} = [Ut^{m+n}, Lt] \subseteq L_{m+n+1}t^{m+n+1},$$

so that $L \subseteq L_{m+n+1}$. It follows that $L_{m+n+1} = L$ for all $m \in \mathbf{N}$, so $\varphi(L(G_{n+2})) = t^{n+2}L[t]$ and hence $L(G_{n+2})$ is contained in $L(H)$. The result follows now from the equivalence in (5.6). □

An immediate corollary of Proposition 5.3.7 is that every non-trivial closed normal subgroup of G has finite index (and hence is open), i.e. G is just infinite.

For two profinite groups H, G we write $H \trianglelefteq_o G$, if H is an open subgroup of G. Let $\{1\} \neq H \trianglelefteq_o G$ be an open normal subgroup, by Proposition 5.3.7 there exists a unique integer $n \in \mathbf{N}$ such that $G_{n+2} < H \leq G_n$ and $H \nsubseteq G_{n+1}$. The ideal $L(H)$ of $L(G)$ is therefore of the form

$$\varphi(L(H)) = L_n t^n \oplus L_{n+1}t^{n+1} \oplus t^n L[t] \tag{5.10}$$

for some non-zero $\mathbf{F}_p$-vector spaces $L_n, L_{n+1} \subseteq L$ and hence $L(H)$ is completely determined by the triple (n, L_n, L_{n+1}). We have $L_n \neq 0$ because $H \nsubseteq G_{n+1}$. Recall that the vector spaces L_n, L_{n+1} are defined by

$$L_{n+1}t^{n+1} = \varphi(HG_{n+1}/G_{n+1}) \quad \text{and} \quad L_{n+1}t^{n+1} = \varphi((H \cap G_{n+1})/G_{n+2}),$$

to simplify the first expression we made use of $G_{n+2} < H \leq G_n$.

Definition 5.3.8. *Let K be a non-Archimedean local field. We define the number δ_K by*

$$\delta_K = \begin{cases} 1 & \text{when } K \text{ is an unramified extension of } \mathbf{Q}_p; \\ 0 & \text{otherwise.} \end{cases}$$

Definition 5.3.9. *Let $n \in \mathbf{N}$ be a positive integer and $V, W \subseteq L$ two $\mathbf{F}_p$-subspaces of L. We call a triplet (n, V, W)* good with respect to *K, if $V \neq 0$ and $\delta_K V + [V, L] \subseteq W$.*

The following lemma shows that there is a relation between L_n and L_{n+1}.

Lemma 5.3.10. *Let L_n, L_{n+1} as in equation* (5.10)*. We then have*

$$\delta_K L_n + [L_n, L] \subseteq L_{n+1}.$$

Proof. Let $\{1\} \neq H \trianglelefteq_o G$ be an open normal subgroup of G with $G_{n+2} < H \leq G_n$ and $H \not\subseteq G_n$. We have $H^p \leq G_{n+1}$ and $(H, G) \leq G_{n+1}$. Since G_{n+1}/G_{n+2} is abelian we find

$$\varphi(H^p G_{n+2}/G_{n+2}) + \varphi((H, G)G_{n+2}/G_{n+2}) = \varphi(H^p(H, G)G_{n+2}/G_{n+2})$$

and the right-hand side is contained in $\varphi((H \cap G_{n+1})/G_{n+2}) = L_{n+1}t^{n+1}$. The group $(H, G)G_{n+2}/G_{n+2}$ is generated by the commutators $(h, g)G_{n+2} = [hG_{n+1}, gG_2]$ for $h \in H$ and $g \in G$ ($hG_{n+1} \in G_n/G_{n+1}$, $gG_2 \in G/G_2$), so we find

$$[HG_{n+1}/G_{n+1}, G/G_2] = (H, G)G_{n+2}/G_{n+2}, \tag{5.11}$$

using that G_{n+1}/G_{n+2} is abelian. Under the isomorphism φ the left-hand side of (5.11) equals $[L_n t^n, Lt] = [L_n, L]t^{n+1}$. If $\delta_K = 0$ we have $H^p \leq G_{n+2}$ by Lemma 5.3.3 and if $\delta_K = 1$ we have by Lemma 5.3.4 that $\varphi(H^p G_{n+2}/G_{n+2}) = \varphi(HG_{n+1}/G_{n+1})t = L_n t^{n+1}$.

□

Remark 5.3.11. By the bilinearity of the bracket $[-, -]$ we have that $[L_n, L]$ is actually a k-subspace of L.

Let H be as above, then the previous lemma shows that we have a map

$$\Phi : \{H \trianglelefteq_o G\} \to \{\text{good triples w.r.t. } K\}, \quad H \mapsto \Phi(H) = (n, L_n, L_{n+1}). \tag{5.12}$$

In the next proposition we show that the map Φ is surjective and we determine the size of any preimage of any given good triplet under the map Φ. In Group Theory the letter Φ is often used to denote the Frattini subgroup of a group. Since we do not work with Frattini subgroups, no confusion should arise.

Proposition 5.3.12. *We use the notation of above and we write $\ell = \dim_{\mathbf{F}_p} L_n$. The map Φ from (5.12) satisfies the following properties:*

(i) Φ is surjective;

(ii) for a good triple (n, L_n, L_{n+1}) with respect to K we have

$$|\Phi^{-1}(n, L_n, L_{n+1})| = |L : L_{n+1}|^{\ell}; \tag{5.13}$$

(iii) if $H \trianglelefteq_o G$ with $\Phi(H) = (n, L_n, L_{n+1})$, then $|G : H| = |L|^{n-1}|L : L_n||L : L_{n+1}|$.

Proof. (i) Let (n, L_n, L_{n+1}) be a triple as in (5.12), we will construct an open normal subgroup $H \trianglelefteq_o G$ such that $\Phi(H) = (n, L_n, L_{n+1})$. Let $a_1, \ldots, a_\ell \in G_n$ be elements such that the $\varphi(a_i G_{n+1})$ form a basis of the vector space $L_n t^n$, moreover let $\varphi(a_{\ell+1}), \ldots, \varphi(a_m) \in$

G_{n+1} be elements such that $\varphi(a_{\ell+1}G_{n+1}), \ldots, \varphi(a_m G_{n+1})$ form a basis of $L_{n+1}t^{n+1}$. Define the group

$$H = \overline{\langle a_1, \ldots, a_m \rangle}^G,$$

the normal closure of the closed subgroup generated by $\{a_1, \ldots, a_m\}$. From the definition of H we immediately see that $H \trianglelefteqslant_c G$, $G_{n+2} < H \leq G_n$ and $H \nsubseteq G_{n+1}$. Because $G_{n+2} \subsetneq H$, we can write $H = \langle a_1, \ldots, a_m \rangle^G G_{n+2}$. From the way we constructed H we see that $\varphi(HG_{n+1}/G_{n+1}) = L_n t^n$ (taking the topological closure doesn't introduce new elements modulo the G_i).
It remains to show that $\varphi((H \cap G_{n+1})/G_{n+2}) = L_{n+1}t^{n+1}$, the "$\supseteq$" follows from the way we constructed H. For "$\subseteq$" we need to show under the map φ that $a_1, \ldots, a_\ell$, their inverses and their G-conjugates do not generate an element outside $L_{n+1}t^{n+1}$. For $n \in \mathbf{N}$ we have

$$((G_n, G_n), G_n) \leq (G_{2n}, G_n) \leq G_{3n} \leq G_{n+2},$$

so the derived subgroup $(G_n, G_n)/G_{n+2}$ is central in G_n/G_{n+2}. Let $g \in G$, then for $1 \leq i \leq \ell$ we have $a_i^g = a_i(a_i, g)G_{n+2}$ with $(a_i, g)G_{n+2} \in (H, G)/G_{n+2}$ central in G_n/G_{n+2}. So for any $x \in H$, which is a product of $a_1, \ldots, a_\ell$, their inverses and their conjugates, we have

$$xG_{n+2} = z \prod_{i=1}^{\ell} a_i^{e_i} G_{n+2}$$

for some integers $e_1, \ldots, e_\ell \in \mathbf{Z}$ and some element $z \in (H, G) \leq G_{n+1}$. If additionally $x \in G_{n+1}$, then we have $p \mid e_i$, because the $\varphi(a_i G_{n+1})$ form a basis of $L_n t^n$. This shows $xG_{n+2} \in H^p(H, G)/G_{n+2}$ and hence

$$\varphi((H \cap G_{n+1})/G_{n+2}) \subseteq \varphi(H^p(H, G)G_{n+2}/G_{n+2}) \subseteq \varphi((H \cap G_{n+1})/G_{n+2}) \subseteq L_{n+1}t^{n+1}.$$

It follows that $\Phi(H) = (n, L_n, L_{n+1})$.

(ii) By Proposition 5.3.7 any subgroup $\{1\} \neq H \trianglelefteqslant_o G$ with $\Phi(H) = (n, L_n, L_{n+1})$ contains the group G_{n+2}, so lifting elements of G_n/G_{n+2} (or equivalently $L_n t^n, L_{n+1}t^{n+1}$) to G_n as in part (i) produces all open normal subgroups of G corresponding to the triple (n, L_n, L_{n+1}).
For the remainder of part (ii) fix a triple (n, L_n, L_{n+1}) as in (5.12) and fix $x_1, \ldots, x_\ell \in G_n$ such that $\varphi(x_1 G_{n+1}), \ldots, \varphi(x_\ell G_{n+1})$ form a basis of $L_n t^n$. Let $\mathbf{a} = (a_1, \ldots, a_\ell) \in G_{n+1}^\ell$ and let $a_{\ell+1}, \ldots, a_m \in G_{n+1}$ be elements such that $\varphi(a_{\ell+1}G_{n+2}), \ldots, \varphi(a_m G_{n+2})$ form a basis of $L_{n+1}t^{n+1}$, then the group

$$H = \overline{\langle a_1 x_1, \ldots, a_\ell x_\ell, a_{\ell+1}, \ldots, a_m \rangle}^G \tag{5.14}$$

satisfies $H \trianglelefteqslant_o G$ and $\Phi(H) = (n, L_n, L_{n+1})$, see part (i). Conversily, every $H \trianglelefteqslant_o G$ with $\Phi(H) = (n, L_n, L_{n+1})$ can be written in this way. It doesn't matter which elements $a_{\ell+1}G_{n+1}, \ldots, a_m G_{n+1}$ we choose (as long as their images under φ form a basis of $L_{n+1}t^{n+1}$)

to define H in (5.14), because any other choice gives rise to the same group H since $G_{n+2} \leq H$. It follows that the group H, defined in (5.14), only depends the tuple $\mathbf{a}$. We therefore write $H_{\mathbf{a}}$ for H. Define a relation $\sim$ on G_{n+1}^{ℓ} by writing $\mathbf{a} \sim \mathbf{b}$, if

$$\varphi(a_i b_i^{-1} G_{n+2}) \in L_{n+1} t^{n+1}, \quad 1 \leq i \leq \ell.$$

Note that $\varphi^{-1}(L_{n+1}t^{n+1}) \trianglelefteqslant G_n/G_{n+2}$ because $(G_n, G_{n+1}) \leq G_{2n+1} \leq G_{n+2}$ for $n \in \mathbf{N}$. The relation $\sim$ is an equivalence relation, being reflexive, symmetric and transitive follows from $L_{n+1}t^{n+1}$ being a group. We show that $\mathbf{a} \sim \mathbf{b}$ if and only if $H_{\mathbf{a}} = H_{\mathbf{b}}$.

- Suppose $H_{\mathbf{a}} = H_{\mathbf{b}}$. For $1 \leq i \leq \ell$ we have $a_i b_i^{-1} = (a_i x_i)(b_i x_i)^{-1} \in H_{\mathbf{a}}$ and hence $\varphi(a_i b_i^{-1} G_{n+2}) \in \varphi((H_{\mathbf{a}} \cap G_{n+1})/G_{n+2}) = L_{n+1}t^{n+1}$ showing that $\mathbf{a} \sim \mathbf{b}$.
- When $\mathbf{a} \sim \mathbf{b}$ we have for $1 \leq i \leq \ell$ that

  $$\varphi(a_i b_i^{-1} G_{n+2}) \in L_{n+1} t^{n+1} = \varphi((H_{\mathbf{a}} \cap G_{n+1})/G_{n+2}),$$

  so there exists a $c_i \in H_{\mathbf{a}} \cap G_{n+1}$ with $a_i G_{n+2} = b_i c_i G_{n+2}$. Together with $G_{n+2} \leq H_{\mathbf{a}}$ this shows that $b_i \in H_{\mathbf{a}}$ for $1 \leq i \leq \ell$, that is $H_{\mathbf{b}} \leq H_{\mathbf{a}}$. Analogously we find $H_{\mathbf{a}} \leq H_{\mathbf{b}}$ and hence $H_{\mathbf{a}} = H_{\mathbf{b}}$.

So far we have established that the number of elements of $\Phi^{-1}(n, L_n, L_{n+1})$ equals the number of equivalence classes of $G_{n+1}^{\ell}/\sim$. The latter is in bijection with tuples of length ℓ of cosets of $L_{n+1}t^{n+1}$ in $\varphi(G_{n+1}/G_{n+2})$, therefore we have

$$|\Phi^{-1}(n, L_n, L_{n+1})| = |(G_{n+1}^{\ell}/\sim)| = |\varphi(G_{n+1}/G_{n+2}) : L_{n+1}t^{n+1}|^{\ell} = |L : L_{n+1}|^{\ell}.$$

(iii) By equation (5.5) we have

$$\begin{aligned} |G : H| &= |L(G) : L(H)| = |\oplus_{i=1}^{n+1} Lt^i : L_n t^n \oplus L_{n+1}t^{n+1}| \\ &= |L|^{n-1} |L : L_n||L : L_{n+1}|. \end{aligned}$$

□

The next example illustrates how two different subgroups of $\mathrm{SL}_2^1(\mathcal{O})$ can have the same good triple with respect to K.

Example 5.3.13. Let π be a uniformiser for the maximal ideal $\mathfrak{p}$ of $\mathcal{O}$ and write $k = \mathcal{O}/\mathfrak{p}$ for the residue field. Let $L = \mathfrak{sl}_2(k)$ be the Lie algebra over k of Chevalley type A_1 with the canonical basis

$$h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

For the group $G = \mathrm{SL}_2^1(\mathcal{O})$, we will construct two different subgroups $H_0, H_1 \trianglelefteqslant_o G$ satisfying $\Phi(H_0) = \Phi(H_1)$. Define the elements $a, b, c, d \in G$ by

$$a = \begin{pmatrix} 1 & \pi \\ 0 & 1 \end{pmatrix}, b = \begin{pmatrix} 1 & \pi^2 \\ 0 & 1 \end{pmatrix}, c = \begin{pmatrix} 1 + \pi^2 + \pi^4 & \pi^2 \\ -\pi^4 & 1 - \pi^2 \end{pmatrix}, d = \begin{pmatrix} 1 & 0 \\ \pi^2 & 1 \end{pmatrix},$$

then $a \in G_1$, $b, c, d \in G_2$ and we have

$$\varphi(aG_2) = xt,\ \varphi(bG_3) = xt^2,\ \varphi(cG_3) = (h+x)t^2,\ \varphi(dG_3) = yt^2.$$

Define the two groups $H_0 = \overline{\langle a, b, c\rangle}^G$ and $H_1 = \overline{\langle da, b, c\rangle}^G$. For $i \in \{0, 1\}$ we compute

$$(H_i \cap G_1)G_2/G_2 = \langle a\rangle G_2/G_2,\ (H_i \cap G_2)G_3/G_3 = \langle b, c\rangle G_3/G_3,$$

with their images under the isomorphism φ are

$$\varphi((H_i \cap G_1)G_2/G_2) = (\mathbf{F}_p x)t,\ \varphi((H_i \cap G_2)G_3/G_3) = (\mathbf{F}_p x + \mathbf{F}_p h)t^2$$

and hence we have

$$\varphi(L(H_0)) = \varphi(L(H_1)) = (\mathbf{F}_p x)t \oplus (\mathbf{F}_p x + \mathbf{F}_p h)t^2 \oplus t^3 L[t].$$

This shows that $\Phi(H_0) = \Phi(H_1)$. Suppose $H_0 = H_1$, then we have $d \in H_0$ and hence $yt^2 \in (\mathbf{F}_p x + \mathbf{F}_p h)t^2$, a contradiction, so $H_0 \neq H_1$.

The next theorem gives a general formula for the normal zeta function for G in terms of the field K and the Lie algebra L. We need the assumption $p \nmid 2d$ in the theorem below, because this whole section is build upon Proposition 5.3.7, which uses Theorem 5.3.5 for which $p \nmid 2d$ is necessary.

Theorem 5.3.14. *Let $d > 1$ be an integer, let p be a prime number with $p \nmid 2d$, let K be a non-Archimedean local field with ring of integers $\mathcal{O}$ and residue class field k with $p = \operatorname{char} k$. The normal zeta function $\zeta_G^{\triangleleft}(s)$ for $G = \mathrm{SL}_d^1(\mathcal{O})$ is given by*

$$\zeta_G^{\triangleleft}(s) = \frac{1}{1 - |L|^{-s}} \sum_{0 \neq V \subseteq L} |L : V|^{-s} \left(\sum_{\delta_K V + [V,L] \subseteq W \subseteq L} |L : W|^{-s + \dim_{\mathbf{F}_p} V} \right),$$

where V, W are $\mathbf{F}_p$-subspaces of L. Here $\delta_K = 1$ if K is an unramified extension of $\mathbf{Q}_p$ and $\delta_K = 0$ otherwise.

Proof. We have seen that the non-trivial open normal subgroups of G are precisely the non-trivial closed normal subgroups of G. To compute the normal zeta function

$$\zeta_G^{\triangleleft}(s) = \sum_{1 \neq H \trianglelefteqslant_o G} |G : H|^{-s},$$

we need, by Proposition 5.3.12, to sum over all good triples with respect to K. If (n, L_n, L_{n+1}) is a good triple with respect to K, then by part (ii) of Proposition 5.3.12 there are

$$|L : L_{n+1}|^{\dim_{\mathbf{F}_p} L_n}$$

subgroups $\{1\} \neq H \trianglelefteq_o G$ such that $\Phi(H) = (n, L_n, L_{n+1})$ and any one of these subgroups satisfies

$$|G : H| = |L|^{n-1}|L : L_n||L : L_{n+1}|$$

by Proposition 5.3.12 (iii). Write $S(K)$ for the set of all good triples with respect to K, then

$$\begin{aligned}
\zeta_G^{\trianglelefteq}(s) &= \sum_{(n,V,W)\in S(K)} |\Phi^{-1}(n,V,W)| \left(|L|^{n-1}|L:V||L:W|\right)^{-s} \\
&= \sum_{n=1}^{\infty} |L|^{-(n-1)s} \sum_{0\neq V\subseteq L} |L:V|^{-s} \left(\sum_{\delta_k V+[V,L]\subseteq W\subseteq L} |\Phi^{-1}(n,V,W)||L:W|^{-s} \right) \\
&= \frac{1}{1-|L|^{-s}} \sum_{0\neq V\subseteq L} |L:V|^{-s} \left(\sum_{\delta_K V+[V,L]\subseteq W\subseteq L} |L:W|^{-s+\dim_{\mathbf{F}_p} V} \right)
\end{aligned}$$

□

5.4 Lie algebra computations

5.4.1 The Lie algebras $\mathfrak{gl}_d(k)$ and $\mathfrak{sl}_d(k)$

Let $d > 1$ be an integer and let k be any field. Write $\mathfrak{gl}_d(k)$ for the Lie algebra $\mathrm{Mat}_d(k)$ of $d \times d$-matrices with entries in k and write $\mathfrak{sl}_d(k) \subseteq \mathfrak{gl}_d(k)$ for the special linear Lie algebra of traceless $d \times d$-matrices over k (Chevalley type A_{d-1}), i.e.

$$\mathfrak{sl}_d(k) = \{x \in \mathfrak{gl}_d(k) \mid \mathrm{Tr}(x) = 0\},$$

both Lie algebras have the usual bracket $[x, y] = xy - yx$ for $x, y \in \mathfrak{gl}_d(k)$.

Let $\mathfrak{g}$ be either the Lie algebra $\mathfrak{gl}_d(k)$ or $\mathfrak{sl}_d(k)$. An element $x \in \mathfrak{g}$ defines the adjoint endomorphism $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}, y \mapsto [x, y]$. The kernel of ad_x is the centraliser

$$C_{\mathfrak{g}}(x) = \{y \in \mathfrak{g} \mid [x, y] = 0\}$$

of x in $\mathfrak{g}$. So $C_{\mathfrak{g}}(x)$ consists of all elements in $\mathfrak{g}$ which commute with x. For a subspace $V \subseteq \mathfrak{g}$ the centraliser $C_{\mathfrak{g}}(V)$ of V inside $\mathfrak{g}$ is defined by

$$C_{\mathfrak{g}}(V) = \bigcap_{x\in V} C_{\mathfrak{g}}(x) = \{y \in \mathfrak{g} \mid xy = yx \text{ for all } x \in V\} \tag{5.15}$$

and moreover we define the subspace

$$[\mathfrak{g}, V] = \sum_{x \in \mathfrak{g}} \mathrm{ad}_x(V) = \mathrm{span}\{[x, y] \mid x \in \mathfrak{g}, y \in V\} \tag{5.16}$$

of $\mathfrak{g}$ spanned by the brackets of elements of $\mathfrak{g}$ with elements of V. Clearly, we may restrict the intersection in (5.15), respectively the summation in (5.16), to run through a basis of V without changing the resulting space. In case V is one-dimensional, the space $C_{\mathfrak{g}}(V)$ is just the centraliser in $\mathfrak{g}$ of any non-zero $x \in V$ and we have $[\mathfrak{g}, V] = \mathrm{ad}_x(\mathfrak{g})$ for any non-zero $x \in V$. Because $[x, y] = -[y, x]$ for $x, y \in \mathfrak{g}$, we have $[\mathfrak{g}, V] = [V, \mathfrak{g}]$. We will write $C_{\mathfrak{gl}}(x), C_{\mathfrak{sl}}(x)$ instead of $C_{\mathfrak{gl}_d(k)}(x), C_{\mathfrak{sl}_d(k)}(x)$ respectively to declutter the notation.

Define on $\mathfrak{g}$ the k-bilinear form $B : \mathfrak{g} \times \mathfrak{g} \to k$ as the ordinary trace form, i.e.

$$B(x, y) = \mathrm{Tr}(xy)$$

for $x, y \in \mathfrak{g}$. The form B satisfies $B(x, [y, z]) = B([x, y], z)$ for all $x, y, z \in \mathfrak{g}$. One can readily check that B is non-degenerate on $\mathfrak{g}$, if $\mathfrak{g} = \mathfrak{gl}_d(k)$ for any field k and if $\mathfrak{g} = \mathfrak{sl}_d(k)$ for any field k satisfying $\mathrm{char}\, k \nmid d$. For the latter claim the trace form B can be represented, with respect to the basis $E_{i,i} - E_{i+1,i+1}$ $(1 \leq i \leq d-1)$, E_{ij}, E_{ji} $(1 \leq i < j \leq d)$ of $\mathfrak{sl}_d(k)$, by the symmetric matrix

$$\begin{pmatrix}
2 & 1 & & & & & & & \\
1 & \ddots & \ddots & & & & & & \\
 & \ddots & \ddots & 1 & & & & & \\
 & & 1 & 2 & & & & & \\
 & & & & 0 & 1 & & & \\
 & & & & 1 & 0 & & & \\
 & & & & & & \ddots & & \\
 & & & & & & & 0 & 1 \\
 & & & & & & & 1 & 0
\end{pmatrix}.$$

With a straightforward induction argument (using a cofactor expansion) one can show that the determinant of the above matrix equals $(-1)^{\frac{d(d-1)}{2}} d$.

We write $V^\perp$ for the orthogonal complement of a subspace $V \subseteq \mathfrak{g}$ with respect to B, so

$$V^\perp = \{x \in \mathfrak{g} \mid B(x, V) = 0\}.$$

The orthogonal complement $V^\perp$ is a subspace of $\mathfrak{g}$. In case B is non-degenerate (i.e. $\mathfrak{g}^\perp = 0$), the dimensions of V and $V^\perp$ are related by

$$\dim V + \dim V^\perp = \dim \mathfrak{g}.$$

One verifies that for two subspaces $V, W \subseteq \mathfrak{g}$ we have

$$V \subseteq W \Leftrightarrow V^{\perp} \supseteq W^{\perp}$$

and in case B is non-degenerate

$$(V^{\perp})^{\perp} = V \quad \text{and} \quad (V \cap W)^{\perp} = V^{\perp} + W^{\perp}.$$

5.4.2 Goal of the computation

Let $d > 1$ be an integer and k a field satisfying char $k \nmid 2d$ (we need this assumption on the characteristic for technical reasons). The goal of our calculations is to understand the two maps $\mathfrak{sl}_d(k) \to \mathfrak{sl}_d(k)$ given by

$$V \mapsto [\mathfrak{sl}_d(k), V] \quad \text{for subspaces} \quad V \subseteq \mathfrak{sl}_d(k) \tag{5.17}$$

and

$$V \mapsto V + [\mathfrak{sl}_d(k), V] \quad \text{for subspaces} \quad V \subseteq \mathfrak{sl}_d(k). \tag{5.18}$$

We want to know how the dimension of $[\mathfrak{sl}_d(k), V]$ and $V + [\mathfrak{sl}_d(k), V]$ depend upon the vector space $V \subseteq \mathfrak{sl}_d(k)$. We are able to do this for $d \in \{2, 3\}$. For $d \geq 4$ the computations become too involved, but we do prove some general results for any $d > 1$. After establishing some general results, we focus on the case $d \in \{2, 3\}$ and later we specialise to the finite field $k = \mathbf{F}_q$. Ultimately this leads to the computation of the numbers $f_q(m, n), g_q(m, n)$, with $1 \leq m, n \leq d^2 - 1$, which count the number of m-dimensional subspaces $V \subseteq \mathfrak{sl}_d(k)$ satisfying $\dim_k [\mathfrak{sl}_d(k), V] = n$, respectively $\dim_k (V + [\mathfrak{sl}_d(k), V]) = n$.

5.4.3 Useful results

We start by summarising some useful results, which we will need later in our calculations. Let $d > 1$ be an integer and let k be a field. Let $\mathfrak{g}$ denote either one of the Lie algebras $\mathfrak{gl}_d(k)$ or $\mathfrak{sl}_d(k)$ and B the ordinary trace form on $\mathfrak{g}$. The first lemma is about the relation between the centralisers in $\mathfrak{gl}_d(k)$ and $\mathfrak{sl}_d(k)$ of any given subspace.

Lemma 5.4.1. *Let $d > 1$ be an integer and k a field satisfying* char $k \nmid d$. *We have $\mathfrak{gl}_d(k) = \mathfrak{sl}_d(k) \oplus k \cdot I$ and for a subspace $V \subseteq \mathfrak{sl}_d(k)$ we have the relation*

$$C_{\mathfrak{gl}}(V) = C_{\mathfrak{sl}}(V) \oplus k \cdot I. \tag{5.19}$$

Consequently, for $x \in \mathfrak{sl}_d(k)$ the dimensions of both centralisers are related by

$$\dim C_{\mathfrak{gl}}(V) = \dim C_{\mathfrak{sl}}(V) + 1.$$

Proof. The condition char $k \nmid d$ implies $I \notin \mathfrak{sl}_d(k)$ and together with the observation that I commutes with every element in $\mathfrak{gl}_d(k)$ the lemma follows. □

We will often work under the assumption char $k \nmid d$ and hence the lemma shows that we do not loose anything by working with $\mathfrak{gl}_d(k)$ instead of $\mathfrak{sl}_d(k)$.

The next lemma shows that the spaces $C_\mathfrak{g}(V)$ and $[\mathfrak{g}, V]$ are related. It provides us with an easy way to compute $[\mathfrak{g}, V]$.

Lemma 5.4.2. *Let $\mathfrak{g}$ and B be as above and assume that B is non-degenerate. For any subspace $V \subseteq \mathfrak{g}$ we have*

$$[\mathfrak{g}, V] = C_\mathfrak{g}(V)^\perp.$$

Proof. We first prove the statement for the 1-dimensional case (the zero-dimensional case is trivial). Let $x \in \mathfrak{g}$ be non-zero, then for $c \in C_\mathfrak{g}(x)$ and all $\ell \in \mathfrak{g}$ we have

$$B([\ell, x], c) = B(\ell, [x, c]) = B(\ell, 0) = 0$$

so $[\mathfrak{g}, x] \subseteq C_\mathfrak{g}(x)^\perp$. The map $\mathrm{ad}_x : \mathfrak{g} \to \mathfrak{g}$ is linear and B is non-degenerate, so

$$\dim C_\mathfrak{g}(x)^\perp = \dim \mathfrak{g} - \dim C_\mathfrak{g}(x) = \dim [\mathfrak{g}, x]$$

and hence $[\mathfrak{g}, x] = C_\mathfrak{g}(x)^\perp$.

For the general case, let $V \subseteq \mathfrak{g}$ be an arbitrary non-zero finite dimensional subspace and let $\{x_i\}_{i \in I}$ be a basis of V, then

$$C_\mathfrak{g}(V)^\perp = \left(\bigcap_{i \in I} C_\mathfrak{g}(x_i) \right)^\perp = \sum_{i \in I} C_\mathfrak{g}(x_i)^\perp = \sum_{i \in I} [\mathfrak{g}, x_i] = [\mathfrak{g}, V]$$

using the result for the 1-dimensional case and that $(U \cap W)^\perp = U^\perp + W^\perp$ for subspaces U, W of $\mathfrak{g}$. □

Remark 5.4.3. The conclusion of Lemma 5.4.2 still holds, if $\mathfrak{g}$ is an arbitrary finite dimensional Lie algebra over k with a non-degenerate k-bilinear form B satisfying $B(x, [y, z]) = B([x, y], z)$ for $x, y, z \in \mathfrak{g}$. For example this holds when $\mathfrak{g}$ is a finite dimensional semisimple Lie algebra over k equipped with the Killing form $\kappa(x, y) = \mathrm{Tr}(\mathrm{ad}_x \circ \mathrm{ad}_y)$ on $\mathfrak{g}$, which is non-degenerate. In case of the Lie algebra $\mathfrak{sl}_d(k)$ we have the relation

$$\kappa(x, y) = 2d \cdot \mathrm{Tr}(xy) \quad \text{for } x, y \in \mathfrak{sl}_d(k) \tag{5.20}$$

and hence the Killing form κ is non-degenerate if and only if char $k \nmid 2d$. Working with the trace form instead of the Killing form on $\mathfrak{sl}_d(k)$ allows us to consider also the case where d is odd and char $k = 2$. Note that when char $k \nmid 2d$ the orthogonal complement will be the same regardless which of the two forms is being used.

The following theorem concerns the double centraliser of an element of $\mathfrak{g}$ for an *arbitrary* field k.

Theorem 5.4.4 (Double centraliser)**.** *Let $d > 1$ be an integer, k an arbitrary field and let $\mathfrak{g}$ be one of the Lie algebras $\mathfrak{gl}_d(k)$ or $\mathfrak{sl}_d(k)$. For $x \in \mathfrak{g}$ we have*

$$C_{\mathfrak{g}}(C_{\mathfrak{g}}(x)) = k[x] \cap \mathfrak{g},$$

here $k[x]$ stands for the subspace of $\mathfrak{gl}_d(k)$ generated by the powers of x (including $x^0 = I$).

The idea of the proof of Theorem 5.4.4 is as follows. We establish the result first for $\mathfrak{gl}_d(k)$. By extension of scalars we may assume that k is algebraically closed, then one shows that the statement is invariant under conjugation by $\mathrm{GL}_d(k)$. This reduces the problem to matrices in Jordan normal form. One then needs to show that the statement can be further reduced to the case of matrices with a single eigenvalue, which, for sake of simplicity, may be assumed to be zero. This is the most cumbersome part of the proof. Finally, the result for $\mathfrak{sl}_d(k)$ can be deduced from the case $\mathfrak{gl}_d(k)$ since $\mathfrak{gl}_d(k) = kI + \mathfrak{sl}_d(k)$.

Lemma 5.4.2 and Theorem 5.4.4 have some useful corollaries, which we need for later calculations. We record them here.

Corollary 5.4.5. *Let $\mathfrak{g}$ be as above and assume that* $\mathrm{char}\ k \nmid d$. *For $x \in \mathfrak{g}$ we have*

$$[\mathfrak{g}, C_{\mathfrak{g}}(x)]^{\perp} = k[x] \cap \mathfrak{g}$$

and hence $\dim [\mathfrak{g}, C_{\mathfrak{g}}(x)] = d^2 - \deg m_x$ *with m_x the minimal polynomial of x over k.*

Proposition 5.4.6. *Let $\mathfrak{g}$ be as above and assume that* $\mathrm{char}\ k \nmid d$. *Let $x \in \mathfrak{g}$, then for any polynomial $p(x) \in k[x]$ we have*

$$[\mathfrak{g}, p(x)] \subseteq [\mathfrak{g}, x];$$

we regard this inclusion as an inclusion inside the Lie algebra $\mathfrak{gl}_d(k)$ (the trace of $p(x)$ is not necessarily zero).

Proof. Consider a polynomial $q(x) \in k[x] \cap \mathfrak{g}$. Using Lemma 5.4.2 and the observation that, if $y \in \mathfrak{g}$ commutes with x, then y also commutes with $q(x)$, we find

$$[\mathfrak{g}, q(x)] = C_{\mathfrak{g}}(q(x))^{\perp} \subseteq C_{\mathfrak{g}}(x)^{\perp} = [\mathfrak{g}, x].$$

Any polynomial $p(x) \in k[x]$ can be written as $p(x) = q(x) + cI$ with $q(x) \in k[x] \cap \mathfrak{g}$ and $c = \frac{1}{d}\mathrm{Tr}(p(x)) \in k$ (note $\mathrm{char}\ k \nmid d$). Therefore

$$[\mathfrak{g}, p(x)] = [\mathfrak{g}, q(x)] + [\mathfrak{g}, cI] = [\mathfrak{g}, q(x)]$$

and the result follows. □

Lemma 5.4.7. *Let $\mathfrak{g}$ be as above and suppose* char $k \nmid d$. *Let $x, y \in \mathfrak{g}$. If we have an inclusion of centralisers $C_{\mathfrak{g}}(x) \subseteq C_{\mathfrak{g}}(y)$, then $y \in k[x] \cap \mathfrak{g}$.*

Proof. From the inclusion $C_{\mathfrak{g}}(x) \subseteq C_{\mathfrak{g}}(y)$ it follows that y commutes with every element in $C_{\mathfrak{g}}(x)$ and hence $y \in C_{\mathfrak{g}}(C_{\mathfrak{g}}(x)) = k[x] \cap \mathfrak{g}$ by Theorem 5.4.4. □

Lemma 5.4.8. *Consider the Lie algebra $\mathfrak{sl}_d(k)$ and assume* char $k \nmid d$. *Suppose $V \subseteq \mathfrak{sl}_d(k)$ is a subspace with $[\mathfrak{sl}_d(k), V] \neq \mathfrak{sl}_d(k)$, then $V \subseteq C_{\mathfrak{sl}}(x)$ for some non-zero $x \in \mathfrak{sl}_d(k)$.*

Proof. Let $f : \mathfrak{sl}_d(k) \to k$ be a linear map with $[\mathfrak{sl}_d(k), V] \subseteq \ker(f)$. Since the bilinear form B is non-degenerate, there exists a non-zero $x \in \mathfrak{sl}_d(k)$ such that $f(y) = B(y, x)$ for all $y \in \mathfrak{sl}_d(k)$. For all $\ell \in \mathfrak{sl}_d(k)$ and all $z \in V$ this gives

$$0 = f([\ell, z]) = B([\ell, z], x) = B(\ell, [z, x]).$$

Because B is non-degenerate, it follows that $[z, x] = 0$ for all $z \in V$ and hence $V \subseteq C_{\mathfrak{sl}}(x)$. □

5.4.4 Jordan normal form and centraliser dimension

We start by recalling some basic facts and notation in connection with the Jordan normal form. Let k be an algebraically closed field and $d \in \mathbf{N}$ a positive integer. A Jordan block of size d with eigenvalue λ is a $d \times d$-matrix of the form

$$\begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}$$

with entries equal to λ on the diagonal, entries equal to 1 on the upper off-diagonal and zeroes everywhere else. The characteristic and minimal polynomial of this Jordan block both equal $(T - \lambda)^d \in k[T]$.

Let $x \in \mathfrak{gl}_d(k)$ be a matrix. The well-known Jordan normal form theorem states that every matrix in $\mathfrak{gl}_d(k)$ is conjugated to a matrix in Jordan normal form. Essentially in a unique way as two different Jordan normal forms of a matrix differ only by permutation of the Jordan blocks. This means that there exist integers $d_1 \geq d_2 \geq \ldots d_p > 0$ satisfying $d_1 + \ldots + d_p = d$, and a corresponding tuple $(\lambda_1, \ldots, \lambda_p) \in k^p$ of eigenvalues of x such that

x is conjugated to the matrix

$$\begin{pmatrix} J(d_1,\lambda_1) & & & \\ & J(d_2,\lambda_2) & & \\ & & \ddots & \\ & & & J(d_p,\lambda_p) \end{pmatrix},$$

here $J(d_i,\lambda_i)$ is a Jordan block of size d_i with eigenvalue λ_i. We call

$$(d_1,\ldots,d_p) \tag{5.21}$$

the *type* of x and note that this is also a partition of d. Knowing the Jordan normal form of a matrix allows us to write down the characteristic and minimal polynomial immediately. The characteristic polynomial $\mathrm{char}_x(T)$ of x is the product of the characteristic polynomials of the $J(d_i,\lambda_i)$, i.e.

$$\mathrm{char}_x(T) = \prod_{i=1}^{p}(T-\lambda_i)^{d_i} \in k[T]$$

and the minimal polynomial $\min_x(T)$ of x is given by

$$\min_x(T) = \mathrm{lcm}\{(T-\lambda_i)^{d_i} \mid 1 \le i \le p\} \in k[T].$$

Moreover, knowing the Jordan normal form of x also determines the dimension of the centraliser $C_{\mathfrak{gl}}(x) = C_{\mathfrak{gl}_d(k)}(x)$ of x in $\mathfrak{gl}_d(k)$. Let $x \in \mathfrak{gl}_d(k)$ be an element with a single eigenvalue and write $(d_1,\ldots,d_p)$ for the type of x. Let $(e_1,\ldots,e_q)$ be the conjugate partition of $(d_1,\ldots,d_p)$, so $e_i = |\{j \mid d_j \ge i\}|$ with $q = d_1$ and $p = e_1$. By [18], Theorem 6.1.3 we have

$$\dim C_{\mathfrak{gl}_d(k)}(x) = \sum_{j=1}^{q} e_j^2. \tag{5.22}$$

When $x \in \mathfrak{gl}_d(k)$ has different eigenvalues $\lambda_1,\ldots,\lambda_\ell$ with $\ell \ge 1$, let x_i be the direct sum of all Jordan blocks of x with eigenvalue λ_i and write n_i for the size of x_i, i.e. $x_i \in \mathrm{Mat}_{n_i}(k)$. We then have

$$\dim C_{\mathfrak{gl}_d(k)}(x) = \sum_{i=1}^{\ell} \dim_{\mathfrak{gl}_{n_i}(k)} C(x_i). \tag{5.23}$$

Let $k' \subseteq k$ be any field. For $x' \in \mathfrak{gl}_d(k')$ we have by extension of scalars that

$$\dim_{k'} C_{\mathfrak{gl}_d(k')}(x') = \dim_k C_{\mathfrak{gl}_d(k)}(x').$$

Starting from $1^2+\ldots+1^2 = d$, $2^2+1^2+\ldots+1^2 = d+2$ and the identity $(m+1)^2 + (n-1)^2 - (m^2+n^2) = 2(m-n)+2$ one can prove the following proposition.

Proposition 5.4.9. *Let $d \in \mathbf{N}$ be a positive integer, let k be any field and let $x \in \mathfrak{gl}_d(k)$ be an element which is not a multiple of the identity matrix. Then we have*

$$\dim C_{\mathfrak{gl}}(x) = d+2m \quad \text{for some integer} \quad 0 \le m \le \tfrac{1}{2}(d-1)(d-2),$$

moreover all of these values arise as centraliser dimensions of elements of $\mathfrak{gl}_d(k)$.

5.4.5 Regular and toxic elements

We distinguish two important types of elements in $\mathfrak{gl}_d(k)$, they are defined in terms of the sizes of their centralisers.

Definition 5.4.10. *Let $d \geq 2$ be an integer. An element $x \in \mathfrak{gl}_d(k)$ is called* regular*, if $\dim C_{\mathfrak{gl}}(x) = d$, the smallest value the dimension of a centraliser can attain. In case* char $k \nmid d$*, we say $x \in \mathfrak{sl}_d(k)$ is* regular*, if $\dim C_{\mathfrak{sl}}(x) = d - 1$. An element $x \in \mathfrak{gl}_d(k)$ is* toxic*, if $\dim C_{\mathfrak{gl}}(x) = (d-1)^2 + 1$, after d^2 the largest value the dimension of a centraliser can attain. In case* char $k \nmid d$*, we say $x \in \mathfrak{sl}_d(k)$ is* toxic*, if $\dim C_{\mathfrak{sl}}(x) = (d-1)^2$.*

As opposed to regular, which is a standard terminology in the literature [7], the notion of toxic is non-standard and was invented by us. Any element in the complement of the regular elements inside the non-zero elements of $\mathfrak{gl}_d(k)$ or $\mathfrak{sl}_d(k)$ is called *irregular*. Some subsets of these irregular elements go sometimes by other names, like sub-regular (see [7]). When char $k \nmid d$ we have $\dim C_{\mathfrak{sl}}(x) = \dim C_{\mathfrak{gl}}(x) - 1$ for $x \in \mathfrak{sl}_d(k)$. Therefore, if $x \in \mathfrak{sl}_d(k)$, then x is regular, respectively toxic, in $\mathfrak{sl}_d(k)$ if and only if x is regular, respectively toxic, in $\mathfrak{gl}_d(k)$. Clearly, being regular or toxic is invariant under conjugation by $\mathrm{GL}_d(k)$ and multiplication by a non-zero scalar.

In the case $d = 2$, all non-zero elements are regular. When $d = 3$, an element is either regular, toxic or zero. The explicit description of the dimension of the centraliser in terms of the sizes of its Jordan blocks can be used to prove the next lemma.

Lemma 5.4.11. *Let $d > 1$ be an integer and let $x \in \mathfrak{gl}_d(k)$ be a toxic element. Then the Jordan normal form of x (up to a permutation of the Jordan blocks) is given by*

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & & & \\ & & \lambda & & \\ & & & \ddots & \end{pmatrix} \quad \textit{or} \quad \begin{pmatrix} \mu & & & & \\ & \lambda & & & \\ & & \ddots & & \\ & & & \lambda & \end{pmatrix}$$

with the eigenvalues $\lambda \neq \mu$ lying in some field extension of k.

The next lemma is concerned with toxic elements in $\mathfrak{sl}_d(k)$ for $d > 2$ (for $d = 2$ there are no toxic elements).

Lemma 5.4.12. *Let $d > 2$ be an integer and k a field with* char $k \neq 2$.

(a) The Jordan normal form (up to a permutation of the Jordan blocks) of a toxic element

in $\mathfrak{sl}_d(k)$ *is*

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & & & \\ & & \lambda & & \\ & & & \ddots & \\ & & & & \lambda \end{pmatrix} \quad or \quad \begin{pmatrix} (1-d)\lambda & & & & \\ & \lambda & & & \\ & & & \ddots & \\ & & & & \lambda \end{pmatrix} \tag{5.24}$$

with $\lambda \in k$ *and* $\lambda \neq 0$ *in the second case. When* $\operatorname{char} k \nmid d$ *we have* $\lambda = 0$ *in the first case.*

(b) A toxic element in $\mathfrak{sl}_d(k)$ *is of the form* $\lambda I + x$ *for some unique* $\lambda \in k$ *and some unique matrix* $x \in \mathfrak{gl}_d(k)$ *of rank 1 satisfying* $d\lambda + \operatorname{Tr}(x) = 0$.

Proof. Part (a) is almost a direct consequence of Lemma 5.4.11. When $x \in \mathfrak{sl}_d(k)$ is conjugate to the first matrix in Lemma 5.4.11, then the minimal polynomial of x is $(T-\lambda)^2 = T^2 - 2\lambda T + \lambda^2 \in k[T]$. Because $\operatorname{char} k \neq 2$ we find $\lambda \in k$. Since $\operatorname{Tr}(x) = 0$ we find $d\lambda = 0$ and when $\operatorname{char} k \nmid d$ we get $\lambda = 0$.

When $x \in \mathfrak{sl}_d(k)$ is conjugate to the second matrix in Lemma 5.4.11, then the condition $\operatorname{Tr}(x) = 0$ gives $\mu + (d-1)\lambda = 0$. Clearly λ is non-zero, because the zero matrix is not toxic. Write $p = \operatorname{char} k$. The minimal and characteristic polynomial of x are

$$(T-\mu)(T-\lambda), (T-\mu)(T-\lambda)^{d-1} \in k[T]$$

respectively. From the minimal polynomial we read off that $(d-2)\lambda, (d-1)\lambda^2 \in k$. If $p \nmid d-2$, then $d-2$ is invertible in k and hence $\lambda \in k$. Suppose $p \mid d-2$, then we get $\lambda^2 \in k$. The idea is now to show that k contains an odd power of λ, which implies $\lambda \in k$. The constant coefficient of the characteristic polynomial gives $(d-1)\lambda^d = \lambda^d \in k$, so if d is odd, then we are done. Assume d is even. Since $d > 2$ we can write $d - 2 = p^n \cdot m$ with $n \geq 1$, $m > 1$, $p \nmid m$ and p odd (if $m = 1$, then $p = 2$, because d is even, which is not possible). The minimal and characteristic polynomial are elements of $k[T]$ and hence so is their quotient $(T-\lambda)^{d-2}$. Expanding this polynomial gives

$$(T-\lambda)^{d-2} = (T^{p^n} - \lambda^{p^n})^m = T^{p^n m} - m\lambda^{p^n} T^{p^n(m-1)} + \ldots,$$

using that $\operatorname{char} k = p$. This shows $m\lambda^{p^n} \in k$. Since $p \nmid m$ and p is odd, we see that k contains an odd power of λ.

(b) That any toxic element in $\mathfrak{sl}_d(k)$ can be written in this form is clear, when the matrix is in Jordan normal form. Conjugating with an invertible matrix leaves λI unchanged and it replaces x with another rank 1 matrix. Hence the statement holds for all toxic elements in $\mathfrak{sl}_d(k)$. The uniqueness of λ, x follows from Corollary 5.5.3. □

Remark 5.4.13. In case the eigenvalues of a toxic element $x \in \mathfrak{sl}_d(k)$ all lie in some Galois extension k' of k, there exists a shorter argument showing that the eigenvalues of x lie in k. Let $\sigma \in \mathrm{Gal}(k'/k)$ be a Galois automorphism of the extension k'/k. If λ is an eigenvalue of a Jordan block of size $m > 0$ of x, then $\sigma(\lambda)$ is also an eigenvalue of a Jordan block of size m of $\sigma(x)$. Since the entries of x are all elements of k, we have $\sigma(x) = x$. Using the description of the Jordan normal form of toxic elements in Lemma 5.4.12(a) it follows that $\sigma(\lambda) = \lambda$ for all $\sigma \in \mathrm{Gal}(k'/k)$ and hence $\lambda \in k$.

5.4.6 Jordan normal forms for $\mathfrak{sl}_3$

Let k be a field and consider the Lie algebra $\mathfrak{sl}_3(k)$. In this section we determine all possible Jordan normal forms for elements of $\mathfrak{sl}_3(k)$.

Proposition 5.4.14. *Let k be a field with* $\mathrm{char}\ k \neq 2, 3$ *and let $\overline{k}$ be an algebraic closure of k. Any matrix of $\mathfrak{sl}_3(k)$ is conjugated by an element of $\mathrm{GL}_3(\overline{k})$ to a matrix in $\mathfrak{sl}_3(\overline{k})$ of the form*

$$i)\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad ii)\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & -2\lambda \end{pmatrix} \text{ or } \quad iii)\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \pi \end{pmatrix},$$

where in ii) we have $\lambda \in k$ and in iii) we have $\lambda, \mu, \pi \in \overline{k}$ (not necessarily distinct) with $\lambda + \mu + \pi = 0$.
Moreover, any toxic element in $\mathfrak{sl}_3(k)$ is conjugated by an element of $\mathrm{GL}_3(k)$ to a matrix in $\mathfrak{sl}_3(k)$ of the form

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & -2\lambda \end{pmatrix}$$

with $\lambda \in k$ non-zero.

Remark 5.4.15. We need to pass to an algebraic closure of k to get a field which contains all the eigenvalues of all the matrices in $\mathfrak{sl}_3(k)$. Note that in iii) the eigenvalues λ, μ, ν lie in a quadratic or a cubic extension of k. Hence, if k is the finite field $\mathbf{F}_q$ with q elements, we can replace in the statement of the lemma the algebraic closure of k with $\mathbf{F}_{q^6}$.

Proof. For $\mathfrak{gl}_3(k)$ the possible Jordan normal forms, up to a permutation of the Jordan blocks, are:

$$i)\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}, \quad ii)\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \mu \end{pmatrix} \text{ and } \quad iii)\begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \pi \end{pmatrix},$$

where the eigenvalues λ, μ, π do not necessarily lie in k. Their respective minimal polynomials are $(T-\lambda)^3$, $\mathrm{lcm}((T-\lambda)^2, (T-\mu)), \mathrm{lcm}((T-\lambda), (T-\mu), (T-\pi)) \in k[T]$.

Passing to $\mathfrak{sl}_3(k)$ we have the extra condition that the trace equals zero. For type i) this gives $\lambda = 0$ (since char $k \neq 3$), for type ii) we see that $\mu = -2\lambda$ and for type iii) we get the condition $\lambda + \mu + \pi = 0$. The characteristic polynomial of an element of type ii) equals

$$T^3 - 3\lambda^2 T + 2\lambda^3 \in k[T]. \tag{5.25}$$

When $\lambda \neq 0$ we find that $\lambda = \frac{3}{2} \cdot \frac{2\lambda^3}{3\lambda^2} \in k$, using that char $k \neq 2, 3$. This shows that all eigenvalues of an element of type ii) lie in k.

From the description of the minimal polynomials (see Lemma 5.4.16), we see that type i) is always regular, type ii) is regular if and only if $\lambda \neq \mu$ and type iii) is regular if and only if λ, μ, π are pairwise different. If an element of type ii) is toxic, then we must have $\lambda = \mu$ forcing $\lambda = 0$ since char $k \neq 3$. Conjugating with the matrix $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{smallmatrix}\right)$ shows that the matrices $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ are similar. Next, if an element of type iii) is toxic, then without loss of generality $\mu = \lambda$ and hence $\pi = -2\lambda$. The characteristic polynomial is then given by the polynomial in (5.25) and hence $\lambda \in k$. □

5.4.7 Number of regular elements in centraliser

Let k be a field, $d > 1$ an integer and consider the Lie algebra $\mathfrak{sl}_d(k)$. We present a lemma, which provides equivalent statements for being regular in $\mathfrak{gl}_d(k)$.

Lemma 5.4.16. *For $x \in \mathfrak{gl}_d(k)$ the following statements are equivalent:*

(a) x is regular in $\mathfrak{gl}_d(k)$ ($\dim C_{\mathfrak{gl}}(x) = d$);

(b) different Jordan blocks of x have different eigenvalues;

(c) $\min_x(T) = \mathrm{char}_x(T)$;

(d) $C_{\mathfrak{gl}}(x) = k[x] = k \cdot I + k \cdot x + \ldots + k \cdot x^{d-1}$.

Proof. (a)⇔(b): Using the formula in (5.22), we have $\dim C_{\mathfrak{gl}}(x) = d$ if and only if in the Jordan normal form of x two different blocks have different eigenvalues.
(b)⇔(c): Suppose that the Jordan blocks of x have sizes $d_1, \ldots, d_m$ (so $d_1 + \ldots + d_m = d$) with corresponding eigenvalues $\lambda_1, \ldots, \lambda_m$ in some algebraic closure of k. The minimal and characteristic polynomial of the Jordan block corresponding to d_i is $(T - \lambda_i)^{d_i}$. The characteristic polynomial of x is given by $\prod_{i=1}^m (T - \lambda_i)^{d_i}$ and the minimal polynomial of x is equal to

$$\mathrm{lcm}\{(T - \lambda_1)^{d_1}, \ldots, (T - \lambda_m)^{d_m}\}.$$

It is now clear that the minimal polynomial of x equals it characteristic polynomial if and only if for $i \neq j$ we have $\lambda_i \neq \lambda_j$.

(d)⇔(c) Suppose $C_{\mathfrak{gl}}(x) = k[x]$. From the inequalities $\dim C_{\mathfrak{gl}}(x) \geq d$ and $\dim k[x] \leq d$ it follows that $\dim C_{\mathfrak{gl}}(x) = d$ and hence the element x is regular which implies that $\min_x(T) = \mathrm{char}_x(T)$. On the other hand, if $\min_x(T) = \mathrm{char}_x(T)$, then the elements $I, x, x^2, \ldots, x^{d-1}$ are linearly independent over k and hence $\dim k[x] = d$ by the theorem of Cayley-Hamilton. Clearly $k[x] \subseteq C_{\mathfrak{gl}}(x)$, from the equivalence of part (a) and (c) it follows that $k[x] = C_{\mathfrak{gl}}(x)$. □

Lemma 5.4.17. *Let k be a field and $x \in \mathfrak{gl}_d(k)$ a regular element. An element $y \in C_{\mathfrak{gl}}(x)$ is regular if and only if y is of the same type (possibly with different eigenvalues, see* (5.21)*) as x, and if there exists a polynomial $f \in k[T]$ of $\deg f < d$ with $y = f(x)$ and*

- *$f(\lambda) \neq f(\mu)$ for different eigenvalues λ, μ of x;*
- *$f'(\lambda) \neq 0$ if λ is an eigenvalue of x with a corresponding Jordan block of size strictly larger than 1.*

Proof. From Lemma 5.4.16 (d) it follows immediately that there exists a polynomial $f \in k[T]$ with $\deg f < d$ such that $y = f(x)$. For the rest of the proof we can assume without loss of generality that k is algebraic closed. Conjugation by an element of $\mathrm{GL}_d(k)$ preserves the dimension of its centraliser, hence we can also assume that x is in Jordan normal form. Write $x = \bigoplus_{i=1}^{p} J(d_i, \lambda_i)$ with $(d_1, \ldots, d_p)$ the type of x and a corresponding tuple $(\lambda_1, \ldots, \lambda_p)$ of eigenvalues of x. From Lemma 5.4.16 (b) we know that the different Jordan blocks of x have different eigenvalues, hence the λ_i are pairwise different. We have

$$y = f(x) = \bigoplus_{i=1}^{p} f(J(d_i, \lambda_i))$$

and using Lemma 5.4.16 we get that y is regular if and only if the Jordan normal form of every matrix $f(J(d_i, \lambda_i))$ has exactly one Jordan block and that no two matrices $f(J(d_i, \lambda_i))$ have the same eigenvalue. The first of the two conditions implies that y has the same type as x. The second condition is equivalent to $f(\lambda) \neq f(\mu)$ for different eigenvalues λ, μ of x, as $f(\lambda_i)$ is the entry on the diagonal of $f(J(d_i, \lambda_i))$.

It remains to show for $d_i > 1$ that the matrix $f(J(d_i, \lambda_i))$ has exactly one Jordan block if and only if the derivative of f at λ_i is non-zero. The Jordan normal form of $f(J(d_i, \lambda_i))$ consists of one block if and only if its minimal polynomial equals its characteristic polynomial $(T - f(\lambda_i))^{d_i}$. A straightforward computation, using that $J(d_i, 0)$ is nilpotent ($J(d_i, 0)^{d_i} = 0$), shows that

$$(f(J(d_i, \lambda_i)) - f(\lambda_i)I)^{d_i - 1} = \begin{pmatrix} 0 & \ldots & 0 & f'(\lambda_i)^{d_i - 1} \\ & & & 0 \\ & & & \vdots \\ & & & 0 \end{pmatrix}$$

and hence the minimal and characteristic polynomial coincide if and only if $f'(\lambda_i) \neq 0$. □

Lemma 5.4.17 gives us a way to compute the number of regular elements in $C_{\mathfrak{gl}}(x)$ when $x \in \mathfrak{gl}_d(k)$ is regular. In case $\operatorname{char} k \nmid d$ the numbers of regular elements in $C_{\mathfrak{sl}}(x)$ and $C_{\mathfrak{gl}}(x)$ for $x \in \mathfrak{sl}_d(k)$ are related, as the following lemma shows.

Lemma 5.4.18. *Suppose $k = \mathbf{F}_q$, the finite field with q elements, with* $\operatorname{char} k \nmid d$. *For every $x \in \mathfrak{sl}_d(k)$ we have*

$$|\{y \in C_{\mathfrak{gl}}(x) \mid y \text{ is regular in } \mathfrak{gl}_d(k)\}| = q \cdot |\{y \in C_{\mathfrak{sl}}(x) \mid y \text{ is regular in } \mathfrak{sl}_d(k)\}|$$

Proof. Suppose that $y \in C_{\mathfrak{gl}}(x)$ is regular in $\mathfrak{gl}_d(k)$, then for any $\lambda \in k$ the element $y + \lambda I$ is also regular in $\mathfrak{gl}_d(k)$. We have $\operatorname{Tr}(y + \lambda I) = \operatorname{Tr}(y) + d\lambda$ and since $\operatorname{char} k \nmid d$ there exists a unique $\lambda \in k$ such that $\operatorname{Tr}(y + \lambda I) = 0$. □

We distinguish five different types of regular elements in $\mathfrak{gl}_3(k)$, with $k = \mathbf{F}_q$, depending on their type and their eigenvalues. Note that for the extension $\mathbf{F}_{q^n}/\mathbf{F}_q$ the map $\alpha \mapsto \alpha^q$ is a generator of the Galois group $\operatorname{Gal}(\mathbf{F}_{q^n}/\mathbf{F}_q)$.

Type	Jordan normal form	Eigenvalues
1a	$\begin{pmatrix} \lambda & & \\ & \mu & \\ & & \pi \end{pmatrix}$	$\lambda, \mu, \pi \in \mathbf{F}_q$ pairwise distinct
1b	$\begin{pmatrix} \lambda & & \\ & \lambda^q & \\ & & \mu \end{pmatrix}$	$\lambda \in \mathbf{F}_{q^2} \backslash \mathbf{F}_q$ and $\mu \in \mathbf{F}_q$
1c	$\begin{pmatrix} \lambda & & \\ & \lambda^q & \\ & & \lambda^{q^2} \end{pmatrix}$	$\lambda \in \mathbf{F}_{q^3} \backslash \mathbf{F}_q$
2	$\begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \mu \end{pmatrix}$	$\lambda, \mu \in \mathbf{F}_q$ different
3	$\begin{pmatrix} \lambda & 1 & \\ & \lambda & 1 \\ & & \lambda \end{pmatrix}$	$\lambda \in \mathbf{F}_q$
4	$\begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \lambda \end{pmatrix}$	$\lambda \in \mathbf{F}_q$
5	$\begin{pmatrix} \lambda & & \\ & \lambda & \\ & & \mu \end{pmatrix}$	$\lambda, \mu \in \mathbf{F}_q$ different

Table 5.1: List of different types of non-zero elements in $\mathfrak{gl}_3(\mathbf{F}_q)$, depending on their Jordan normal form and their eigenvalues.

Lemma 5.4.19. *Let* $\mathbf{F}_q$ *be the finite field of cardinality* q *with* $\operatorname{char} \mathbf{F}_q \neq 2, 3$. *Table 5.2 displays for each type of regular element* $x \in \mathfrak{sl}_3(\mathbf{F}_q)$, *the number of regular elements in* $C_{\mathfrak{sl}}(x)$.

Type of x	$\lvert C_{\mathfrak{sl}}(x) \cap \{\text{regular}\}\rvert$
1a	$(q-1)(q-2)$
1b	q^2-q
1c	q^2-1
2	$(q-1)^2$
3	q^2-q

Table 5.2: For each type of regular element in $x \in \mathfrak{sl}_3(\mathbf{F}_q)$ we record the number of regular elements in $C_{\mathfrak{sl}}(x)$.

Proof. We compute for each type of regular element $x \in \mathfrak{gl}_3(\mathbf{F}_q)$ the number of regular elements in $C_{\mathfrak{gl}}(x)$, Lemma 5.4.18 then gives the result for $\mathfrak{sl}_3(\mathbf{F}_q)$.

For type 1a the centraliser is computed to be

$$\left\{ \left(\begin{smallmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{smallmatrix} \right) \mid a, b, c \in \mathbf{F}_q \right\}.$$

Any such matrix is regular if and only if it has different elements on the diagonal, hence there are $q(q-1)(q-2)$ such matrices.

For type 1b we use Lemma 5.4.17, so we need to compute the number of quadratic polynomials $f(T) = aT^2+bT+c \in \mathbf{F}_q[T]$ such that $f(\lambda), f(\lambda^q), f(\mu)$ are pairwise different. Because $\alpha \mapsto \alpha^q$ is an element of the Galois group $\operatorname{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$ and $\mu \in \mathbf{F}_q$ is fixed by any element of $\operatorname{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$, we have $f(\lambda) \neq f(\mu)$ if and only if $f(\lambda^q) \neq f(\mu)$. Hence the elements $a, b \in \mathbf{F}_q$ need to satisfy $a(\lambda+\mu)+b, a(\lambda+\lambda^q)+b \neq 0$. If $a = 0$ we get $b \neq 0$, giving $q(q-1)$ polynomials, and if $a \neq 0$ we find $b \neq -a(\lambda+\lambda^q) \in \mathbf{F}_q$, giving $q(q-1)^2$ polynomials. In total we find q^3-q^2 different polynomials $f \in \mathbf{F}_q[T]$ such that $f(\lambda), f(\lambda^q), f(\mu)$ are pairwise different.

For type 1c we use again Lemma 5.4.17, so we need to compute the number of quadratic polynomials $f(T) = aT^2+bT+c \in \mathbf{F}_q[T]$ such that $f(\lambda), f(\lambda^q), f(\lambda^{q^2})$ are pairwise different. Because $\alpha \mapsto \alpha^q$ is an element of the Galois group $\operatorname{Gal}(\mathbf{F}_{q^3}/\mathbf{F}_q)$ this is equivalent to $f(\lambda) \neq f(\lambda^q)$ and that holds if and only if $a(\lambda+\lambda^q)+b \neq 0$. We have $\lambda^{q^2} \notin \mathbf{F}_q$ because $\lambda \in \mathbf{F}_{q^3} \backslash \mathbf{F}_q$ and hence since $\lambda+\lambda^q+\lambda^{q^2} \in \mathbf{F}_q$ we have $\lambda+\lambda^q \notin \mathbf{F}_q$. If $a = 0$ we get $b \neq 0$, giving $q(q-1)$ polynomials, and if $a \neq 0$ we may choose b, c freely since $\lambda+\lambda^q \notin \mathbf{F}_q$, giving $q^2(q-1)$ polynomials. In total we find q^3-q different polynomials $f \in \mathbf{F}_q[T]$ such that $f(\lambda), f(\lambda^q), f(\lambda^{q^2})$ are pairwise different.

For type 2 the centraliser is given by

$$\left\{ \begin{pmatrix} a & b & 0 \\ 0 & a & 0 \\ 0 & 0 & c \end{pmatrix} \mid a, b, c \in \mathbf{F}_q \right\}.$$

Clearly we need $b \neq 0$ and $c \neq a$, otherwise different Jordan blocks have the same eigenvalue. Under these assumptions the matrix is regular, its minimal polynomial is seen to be $(T-a)^2(T-c)$. It follows that this centraliser contains $q(q-1)^2$ different regular elements.

For type 3 the centraliser is computed to be

$$\left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \mid a, b, c \in \mathbf{F}_q \right\}. \tag{5.26}$$

Write x for the matrix displayed in (5.26). If $b = 0$, then the minimal polynomial divides $(T-a)^2$ and hence x is not regular, and if $b \neq 0$ we compute $(x-aI)^2 = \begin{pmatrix} 0 & 0 & b^2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, which is non-zero, so the minimal polynomial doesn't divide $(T-a)^2$ and hence x is regular. This shows that this centraliser contains $q^2(q-1)$ different regular elements. □

5.5 Properties of rank-1 matrices

Let $d > 0$ be an integer and k some field. In this section we record some properties of rank 1 matrices in $\mathfrak{gl}_d(k)$. We will need them in the next section. For integers $m, n > 0$ we denote the transpose of a matrix $x \in \mathrm{Mat}_{mn}(k)$ by $x^T \in \mathrm{Mat}_{nm}(k)$ and we write $k^n = \mathrm{Mat}_{n1}(k)$.

Lemma 5.5.1. *Let $d > 0$ be an integer, let k be a field and let $x, y \in \mathfrak{gl}_d(k)$ be two matrices of rank 1.*

(a) There exist non-zero $a, b \in k^d$ such that $x = ab^T$. Every other non-zero $a', b' \in k^d$ with $x = a'b'^T$ satisfy $a' = \lambda a$ and $b' = \lambda^{-1}b$ for some $\lambda \in k^*$.

(b) Assume that $d \geq 3$. If $\mathrm{rank}(\lambda I + x) = 1$ for some $\lambda \in k$, then $\lambda = 0$.

(c) Assume that $d \geq 3$ and let $\lambda, \mu \in k$. If $\mathrm{char}\ k \nmid d$ and $\lambda I + x, \mu I + y \in \mathfrak{sl}_d(k)$, then $\lambda I + x$, $\mu I + y$ are linearly dependent in $\mathfrak{gl}_d(k)$ if and only if $y = cx$ for some $c \in k^*$. The latter is equivalent to the row and column spaces of x and y being equal.

(d) If $\mathrm{rank}(x + y) = 1$, then the matrices x and y have the same row space or the same column space (but not necessarily both).

Proof. For $1 \leq i \leq d$ we write $e_i \in k^d$ for the i-th unit vector.

(a) Let $a \in k^d$ be an element spanning the 1-dimensional column space of x. For each $1 \leq i \leq d$ let $b_i \in k$ be the unique scalar such that $xe_i = b_i a$. Define $b = (b_1, \ldots, b_d)^T \in k^d$.

Then we see that x can be written as $x = ab^T$. Since x is non-zero so are a, b. Starting with another $a' \in k^d$, so $a' = \lambda a$ for some $\lambda \in k^*$, produces by the formula $xe_i = b'_i a'$ an element $b' = \lambda^{-1} b$.

(b) We have the following inequality,

$$\operatorname{rank}(\lambda I) = \operatorname{rank}(\lambda I + x - x) \leq \operatorname{rank}(\lambda I + x) + \operatorname{rank}(x) = 2,$$

and since $d \geq 3$ we see that $\lambda = 0$.

(c) If $\lambda I + x$ and $\mu I + y$ are linearly dependent in $\mathfrak{gl}_d(k)$, then there exists $c \in k^*$ such that $c(\lambda I + x) = \mu I + y$, i.e. $(c\lambda - \mu)I + cx = y$. Using part (b), we see that $\mu = c\lambda$ and hence $cx = y$. For the other direction, we have $d\lambda + \operatorname{Tr}(x) = d\mu + \operatorname{Tr}(y) = 0$ and hence

$$\mu I + y = -\tfrac{\operatorname{Tr}(y)}{d} I + y = c(-\tfrac{\operatorname{Tr}(x)}{d} I + x) = c(\lambda I + x).$$

(d) Assume that the column spaces of x and y are different. The rank of $x + y$ does not change under an invertible linear transformation, so after applying an invertible transformation sending the column spaces of x, y to respectively $\langle e_1 \rangle$ and $\langle e_2 \rangle$, we may assume that the column spaces of x, y are spanned by respectively e_1, e_2. By part (a) we can write $x = e_1 a^T$ and $y = e_2 b^T$ for some non-zero $a, b \in k^d$. It follows that the row space of $x + y$ is spanned by a^T and b^T. Since $x + y$ has rank 1, the elements a, b are linearly dependent and hence the row spaces of x and y coincide. □

Definition 5.5.2. *Let $d > 0$ be an integer and let k be a field. A rank-1 matrix $x \in \mathfrak{gl}_d(k)$ can be written as $x = ab^T$ for non-zero $a, b \in k^d$ by Lemma 5.5.1 with uniqueness up to a multiple by a non-zero scalar. The row space and the column space of x are denoted by* $\operatorname{row}(x) = \langle a \rangle$, $\operatorname{col}(x) = \langle b \rangle$ *respectively .*

Part (b) of Lemma 5.5.1 has the following corollary, which we already saw (under the assumption char $k \neq 2$ in Lemma 5.4.12).

Corollary 5.5.3. *Let $d > 2$ be an integer and let k be a field. If $\lambda I + x \in \mathfrak{sl}_d(k)$ is a toxic element with $\lambda \in k$ and x a rank-1 matrix, then λ and x are uniquely determined up to a multiple by a non-zero scalar.*

Proof. Suppose $\lambda I + x = \mu I + y$ with $\lambda, \mu \in k$ and $x, y \in \mathfrak{gl}_d(k)$ two rank 1 matrices, then $(\lambda - \mu)I + x = y$ and so by part (b) of Lemma 5.5.1 we have $\lambda = \mu$ and consequently $x = y$. □

5.6 Toxic subspaces

Lemma 5.6.1. *Let $d > 2$ be an integer and let k be a field with* char $k \nmid 2d$. *The Lie algebra homomorphism $\varphi : \mathfrak{gl}_d(k) \to \mathfrak{sl}_d(k), x \mapsto x - \frac{\mathrm{Tr}(x)}{d} I$ induces a bijection*

$$\{x \in \mathfrak{gl}_d(k) \mid \mathrm{rank}(x) = 1\} \mapsto \{\text{toxic elements of } \mathfrak{sl}_d(k)\}$$
$$x \mapsto x - \frac{\mathrm{Tr}(x)}{d} I.$$

Proof. A straightforward verification shows that φ is indeed a Lie algebra homomorphism with kernel $\ker \varphi = \{cI \mid c \in k\}$. If $x \in \mathfrak{gl}_d(k)$ has rank 1, then the matrix x satisfies $x^2 = \mathrm{Tr}(x)x$ and hence the eigenvalues of x are 0 (with multiplicity at least $d-1$) and $\mathrm{Tr}(x)$ (with multiplicity at most 1). Up to conjugation by an element of $\mathrm{GL}_d(k)$ and up to multipication by some scalar in k^* the matrix x is therefore equal to

$$\begin{pmatrix} 1 & & \\ & 0 & \\ & & \ddots \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 1 & \\ & 0 & \\ & & \ddots \end{pmatrix}.$$

The images of these two matrices under φ are of the form as described in Lemma 5.4.12. Conjugating and multiplying by a non-zero scalar does not change the centraliser dimension, hence the images are toxic elements in $\mathfrak{sl}_d(k)$. Conversely, by part (b) of Lemma 5.4.12 every toxic element in $\mathfrak{sl}_d(k)$ is of the form $\lambda I + x$ with $\lambda \in k$ and $x \in \mathfrak{gl}_d(k)$ a rank 1 matrix. Since $d\lambda + \mathrm{Tr}(x) = 0$ we see that $\lambda I + x = \varphi(x)$. The injectivity follows from Corollary 5.5.3. □

Definition 5.6.2. *Let $d > 2$ be an integer, let k be a field and let $\mathfrak{g}$ denote either $\mathfrak{gl}_d(k)$ or $\mathfrak{sl}_d(k)$. A non-zero subspace $V \subseteq \mathfrak{g}$ with every non-zero element being regular (resp. toxic) is called a* regular subspace *(resp.* toxic subspace*) of $\mathfrak{g}$.*

The next lemma is a key ingredient of Theorem 5.6.4 below.

Lemma 5.6.3. *Let $d \geq 3$ be an integer, let k be a field with at least three elements and suppose that* char $k \nmid d$. *Write φ for the Lie algebra homomorphism of Lemma 5.6.1. Let $V \subseteq \mathfrak{sl}_d(k)$ be a toxic subspace and let $x, y \in \mathfrak{gl}_d(k)$ be two rank-1 matrices with $\varphi(x), \varphi(y) \in V$. Then the row spaces of x and y or the column spaces of x and y coincide.*

Proof. Assume that the column spaces of x and y are different; without loss of generality we may assume that they are spanned by e_1 and e_2 respectively. By Lemma 5.5.1 there exist $a, b \in k^d$ such that $x = e_1 a^T$ and $y = e_2 b^T$. For $\alpha, \beta \in k$ we have

$$\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y) \in V.$$

Because V is toxic and φ induces a bijection between rank-1 matrices and toxic elements by Lemma 5.6.1, there exists a unique rank-1 matrix $z \in \mathfrak{gl}_d(k)$ (depending on α, β) such that $\varphi(\alpha x + \beta y) = \varphi(z)$ and hence $z = tI + \alpha x + \beta y$ where $t = t(\alpha, \beta) \in k$ is a scalar depending also on α, β. Because z has rank 1 all 2×2-minors of z vanish, in particularly because $d \geq 3$ this gives

$$t(t + \beta b_2) = t(t + \alpha a_1) = 0.$$

If for all $\alpha, \beta \neq 0$ we have $t \neq 0$, then we see that the equation $\alpha a_1 = \beta b_2$ holds for all $\alpha, \beta \neq 0$. Setting $\alpha = \beta = 1$ gives $a_1 = b_2$ and then $\alpha = 1$ and $\beta \in k \backslash \{0, 1\}$ gives $(\beta - 1)b_2 = 0$, hence $b_2 = 0$. It follows that $t^2 = 0$ for all $\alpha, \beta \neq 0$, a contradiction.
If for some $\alpha, \beta \neq 0$ we have $t = 0$, then $z = \alpha x + \beta y$. By Lemma 5.5.1(d) the row or the column spaces of αx and of βy coincide and hence, since α, β are non-zero and we assumed that $\mathrm{col}(x) \neq \mathrm{col}(y)$, we conclude that the row spaces of x and y are the same. □

Theorem 5.6.4. *Let $d \geq 3$ be an integer, let k be a field with $\mathrm{char}\, k \nmid d$ and let φ be the map from Lemma 5.6.1. For an ℓ-dimensional toxic subspace $V \subseteq \mathfrak{sl}_d(k)$ there exist unique subspaces $U, W \subseteq k^d$ with $\dim U = \ell$ and $\dim W = 1$ such that*

$$V = \varphi(UW^T) \quad \text{or} \quad V = \varphi(WU^T),$$

here $\varphi(UW^T) = \{uw^T \mid u \in U, w \in W\}$ and similar for $\varphi(WU^T)$, and consequently we have $\ell \leq d$. For $1 \leq \ell \leq d$ we have

$$\dim [\mathfrak{sl}_d(k), V] = (d - 1)(\ell + 1).$$

Note that when $\ell = 1$ the second possibility is obsolete, as both spaces U, W have dimension 1.

Proof. Because $\dim V = \ell$ there exist by Lemma 5.6.1 ℓ rank-1 matrices $x_1, \ldots, x_\ell \in \mathfrak{gl}_d(k)$ such that $\varphi(x_1), \ldots, \varphi(x_\ell)$ form a basis of V. By Lemma 5.6.3 we have for each pair of integers $1 \leq i, j \leq \ell$ with $i \neq j$ that the row spaces or the column spaces of x_i and x_j coincide. It follows that $x_1, \ldots, x_\ell$ all have the same row space or the same column space; without loss of generality we assume it is the row space.

From Lemma 5.5.1(a) it follows that $\ell \leq d$. Any element of V is for some $a_i \in k$ of the form $\sum_{i=1}^{\ell} a_i \varphi(x_i) = \varphi(\sum_{i=1}^{\ell} a_i x_i)$. Since all x_i share the same row space, the rank of $\sum_{i=1}^{\ell} a_i x_i$ is at most one. It follows that we must have $U = \sum_{i=1}^{\ell} \mathrm{col}(x_i)$ and $W = \mathrm{row}(x_1)$.

Next, we prove the formula for $\dim[\mathfrak{sl}_d(k), V]$. After conjugating with a suitable matrix from $\mathrm{GL}_d(k)$ we may assume without loss of generality that $V = \varphi(UW^T)$ where $U = \langle e_1, \ldots, e_\ell \rangle \subseteq k^d$ and $W = \langle a \rangle$ with $a = (a_1, \ldots, a_d) \in k^d$ non-zero. Let $x = (x_{ij})_{1 \leq i,j \leq d} \in$

$C_{\mathfrak{sl}}(V) = \bigcap_{1\leq i\leq \ell} C_{\mathfrak{sl}}(e_i a^T)$ be a matrix with columns $c_1, \ldots, c_d \in k^d$. For $1 \leq i \leq \ell$ we have

$$\begin{pmatrix} a_1x_{1i} & \ldots & a_dx_{1i} \\ \vdots & & \vdots \\ a_1x_{di} & \ldots & a_dx_{di} \end{pmatrix} = c_i a^T = xe_i a^T = e_i a^T x = e_i(a^T c_1, \ldots, a^T c_d) = \begin{pmatrix} a^T c_1 & \ldots & a^T c_d \\ & & \end{pmatrix},$$

in the matrix on the right we have displayed the i-th row and all other entries of this matrix are zero. For fixed $1 \leq i \leq \ell$ it follows that $x_{mi} = 0$ for every $m \neq i$ and $a_j x_{ii} = a^T c_j$ for all $1 \leq j \leq d$. Let j be such that $a_j \neq 0$, then for any $1 \leq i \leq \ell$ we have $a_j x_{11} = a^T c_j = a_j x_{ii}$ and hence $x_{11} = x_{ii}$, showing that $x_{11} = \ldots = x_{\ell\ell}$. So $x \in C_{\mathfrak{sl}}(V)$ is equivalent to the columns of x satisfying the following conditions: for $1 \leq i \leq \ell$ we have $c_i = x_{11}e_i$, for $\ell + 1 \leq i \leq d$ we have $a_i x_{11} = a^T c_i$, a non-trivial linear dependency between $x_{11}, x_{1i}, \ldots, x_{di}$, and $\mathrm{Tr}(x) = 0$. Consequently, the dimension of $C_{\mathfrak{sl}}(V)$ is given by

$$\dim C_{\mathfrak{sl}}(V) = 1 + (d-\ell)(d-1) - 1 = (d-\ell)(d-1)$$

and therefore by Lemma 5.4.2 we have

$$\begin{aligned} \dim[\mathfrak{sl}_d(k), V] &= \dim C_{\mathfrak{sl}}(V)^\perp = \dim \mathfrak{sl}_d(k) - \dim C_{\mathfrak{sl}}(V) \\ &= d^2 - 1 - (d-1)(d-\ell) = (d-1)(\ell+1). \end{aligned}$$

Let $0 \neq a = (a_1, \ldots, a_d) \in k^d$, let $U \subseteq k^d$ with $\dim U = \ell$ and $W = k \cdot a$ be subspaces of $\mathfrak{sl}_d(k)$. The space $V = \varphi(UW^T)$ is an example of a toxic ℓ-dimensional space. Namely, UW^T is a subspace of $\mathfrak{gl}_d(k)$ in which every element has rank 1, by Lemma 5.6.1 every non-zero element in $\varphi(V)$ is toxic. □

5.6.1 On the identity $[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), x]] = \mathfrak{sl}_d(k)$

In this section we will prove the following theorem.

Theorem 5.6.5. *Let $d > 1$ be an integer and let k be a field satisfying* $\mathrm{char}\ k \nmid d$. *For the Lie algebra $\mathfrak{g} = \mathfrak{sl}_d(k)$ we have the identity*

$$[\mathfrak{g}, [\mathfrak{g}, x]] = \mathfrak{g}$$

for all non-zero $x \in \mathfrak{g}$, except when $\mathrm{char}\ k = 2$ *and $x^2 = 0$ in which case we have*

$$[\mathfrak{g}, [\mathfrak{g}, [\mathfrak{g}, x]]] = \mathfrak{g}.$$

Remark 5.6.6. The assumption that $\mathrm{char}\ k \nmid d$ is necessary for the statement of Theorem 5.6.5 to hold for all elements of $\mathfrak{sl}_d(k)$. For example, if $\mathrm{char}\ k \mid d$, then taking the identity element $I \in \mathfrak{sl}_d(k)$ we see that $[\mathfrak{sl}_d(k), I] = 0$ and hence $[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), I]] = 0$ as well. In case $\mathrm{char}\ k = 2$ the statement of Theorem 5.6.5 also holds for almost all elements of $\mathfrak{sl}_d(k)$, see Proposition 5.6.12 for more details. In any case we need to take the bracket at least twice by Lemma 5.4.2.

Lemma 5.6.7. *Let $d > 1$ be an integer and let k be a field satisfying* $\operatorname{char} k \nmid d$. *For any element $x \in \mathfrak{sl}_d(k)$ we have $[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), x]] = \mathfrak{sl}_d(k)$ if and only if*

$$C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp}) = k \cdot I \tag{5.27}$$

and similarly $[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), x]]] = \mathfrak{sl}_d(k)$ if and only if $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp})^{\perp}) = k \cdot I$.

Proof. Because $\operatorname{char} k \nmid d$, the trace form is non-degenerate on $\mathfrak{sl}_d(k)$. Let $x \in \mathfrak{sl}_d(k)$. Using Lemma 5.4.2, the identity $[\mathfrak{sl}_d(k), [\mathfrak{sl}_d(k), x]] = \mathfrak{sl}_d(k)$ is equivalent to

$$C_{\mathfrak{sl}}(C_{\mathfrak{sl}}(x)^{\perp}) = 0. \tag{5.28}$$

We will show that the statements (5.28) and (5.27) are equivalent. The trace form on $\mathfrak{gl}_d(k)$ restricts to a non-degenerate form on $\mathfrak{sl}_d(k)$ (because $\operatorname{char} k \nmid d$). Using that $C_{\mathfrak{sl}}(x) = \mathfrak{sl}_d(k) \cap C_{\mathfrak{gl}}(x)$ for $x \in \mathfrak{sl}_d(k)$, we see that inside $\mathfrak{gl}_d(k)$ the statement (5.28) is equivalent to

$$\mathfrak{sl}_d(k) \cap C_{\mathfrak{gl}}(\mathfrak{sl}_d(k) \cap (\mathfrak{sl}_d(k) \cap C_{\mathfrak{gl}}(x))^{\perp}) = 0. \tag{5.29}$$

Because $\operatorname{char} k \nmid d$ we have for $x \in \mathfrak{sl}_d(k)$ that

$$C_{\mathfrak{gl}}(x) = k \cdot I \oplus C_{\mathfrak{sl}}(x) \quad \text{and} \quad (k \cdot I)^{\perp} = \mathfrak{sl}_d(k),$$

and hence

$$\begin{aligned} C_{\mathfrak{gl}}(x)^{\perp} &= (k \cdot I \oplus C_{\mathfrak{sl}}(x))^{\perp} = (k \cdot I)^{\perp} \cap C_{\mathfrak{sl}}(x)^{\perp} \\ &= \mathfrak{sl}_d(k) \cap (\mathfrak{sl}_d(k) \cap C_{\mathfrak{gl}}(x))^{\perp}. \end{aligned}$$

It follows that (5.29), and hence (5.28), is equivalent to

$$\mathfrak{sl}_d(k) \cap C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp}) = 0. \tag{5.30}$$

Since $I \notin \mathfrak{sl}_d(k)$ it is clear that (5.27) implies (5.30). Conversely, if (5.30) holds, then combining this with $\mathfrak{gl}_d(k) = k \cdot I \oplus \mathfrak{sl}_d(k)$ and $k \cdot I \subseteq C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp})$, it follows that (5.27) holds. The second part of Lemma 5.6.7 can be proved in an analogous way. □

The next two lemmas contain some well-known results or straightforward verifiable statements. Consequently, we do not provide a proof. We need the two lemmas for the proof of Theorem 5.6.5.

Lemma 5.6.8. *Let $d \in \mathbf{N}$ be a positive integer and let k be a field. Write $e_{mn} \in \mathfrak{gl}_d(k)$ for the elementary matrix with an entry 1 in position (m, n) and all other entries equal to 0. We have $x = (x_{ij}) \in C_{\mathfrak{gl}}(e_{mn})$ if and only if $x_{n\ell} = 0$ for all $\ell \neq n$, $x_{\ell m} = 0$ for all $\ell \neq m$ and $x_{mm} = x_{nn}$.*

Remark 5.6.9. The second part of Lemma 5.6.8 can be rephrased as: all entries in the n-th row and the m-th column of x, except for the entries on the diagonal, are zero and the m-th and n-th entry on the diagonal are equal.

Lemma 5.6.10. *Let $m, n \in \mathbf{N}$ be positive integers and let k be a field. Let $a \in \mathfrak{gl}_m(k), b \in \mathfrak{gl}_n(k)$ be two Jordan blocks and suppose that $x = (x_{i,j}) \in \mathrm{Mat}_{mn}(k)$ satisfies $ax = xb$. If*

(a) a and b have different eigenvalues, then $x = 0$;

(b) a and b have the same eigenvalues and $m \geq n$, then $x_{i,j} = 0$ if $j < i$ and $x_{i,j} = x_{i+1,j+1}$ for $i \leq j$ with $1 \leq i \leq m-1$ and $1 \leq j \leq n-1$.

(c) a and b have the same eigenvalues and $m < n$, then $x_{i,j} = 0$ if $j \leq i$ and $x_{i,j} = x_{i+1,j+1}$ for $i < j$ with $1 \leq i \leq m-1$ and $1 \leq j \leq n-1$.

Remark 5.6.11. The second part of Lemma 5.6.8 (b) can be rephrased as: all entries below the diagonal of x are zero and on every off diagonal (including the diagonal itself) the entries are equal.

In the next proposition we prove an identity, from which the statements in Lemma 5.6.7 and hence Theorem 5.6.5 follow.

Proposition 5.6.12. *Let $d > 1$ be an integer and let k be a field with* char $k \nmid d$. *For $x \in \mathfrak{gl}_d(k)$ with $x \notin k \cdot I$ the identity*

$$C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp}) = k \cdot I \tag{5.31}$$

holds, except if in the case where x has one eigenvalue λ with $(x-\lambda I)^2 = 0$ and char $k = 2$. *In the latter case we have $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp}) = k \cdot I \oplus k \cdot x$ and $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp})^{\perp}) = k \cdot I$.*

Proof. The inclusion "$\supseteq$" clearly holds, so it remains to prove the other direction. The space $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x))^{\perp}$ is a vector space defined over k, so it is enough to prove the identity in (5.31) for algebraically closed fields k (the dimension of $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x))^{\perp}$ doesn't change, when extending scalars to a field extension of k). So without loss of generality assume that k is algebraically closed. For $g \in \mathrm{GL}_d(k)$ we have

$$C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(gxg^{-1}))^{\perp} = gC_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x))^{\perp}g^{-1}$$

and hence we may also assume without loss of generality that x is in Jordan normal form. The proof is now divided into two parts, depending on whether x has one single eigenvalue or at least two different eigenvalues.

First, assume that x has at least two different eigenvalues. Let $a \in \mathfrak{gl}_m(k), b \in \mathfrak{gl}_n(k)$ be two square matrices in Jordan normal form without a common eigenvalue, write $x = \left(\begin{smallmatrix} a & O \\ O & b \end{smallmatrix}\right)$.

By Lemma 5.6.10(a) the Jordan blocks (of possible different sizes) with different eigenvalues do not commute. Therefore

$$C_{\mathfrak{gl}}(x) = \left(\begin{smallmatrix} C_{\mathfrak{gl}}(a) & O \\ O & C_{\mathfrak{gl}}(b) \end{smallmatrix} \right)$$

For $a' \in C_{\mathfrak{gl}}(a)$, $b' \in C_{\mathfrak{gl}}(b)$ and arbitrary $y \in \mathrm{Mat}_{mn}(k)$, $z \in \mathrm{Mat}_{nm}(k)$, we have

$$\mathrm{Tr}\left(\left(\begin{smallmatrix} a' & O \\ O & b' \end{smallmatrix} \right) \left(\begin{smallmatrix} O & y \\ z & O \end{smallmatrix} \right) \right) = \mathrm{Tr}\left(\begin{smallmatrix} O & a'y \\ b'z & O \end{smallmatrix} \right) = 0$$

and hence $\left(\begin{smallmatrix} O & * \\ * & O \end{smallmatrix} \right) \subseteq C_{\mathfrak{gl}}(x)^{\perp}$. This gives $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp}) \subseteq C_{\mathfrak{gl}}\left(\begin{smallmatrix} O & * \\ * & O \end{smallmatrix} \right) = k \cdot I$, the latter equality follows from applying Lemma 5.6.8.

Next, assume that x has only a single eigenvalue and that the Jordan blocks of x appear in descending order (the largest Jordan block appears in the upper left corner). Write e for the size of the largest Jordan block of x and ℓ for the number of Jordan blocks of x of size e. Then $e > 1$ because x is not a scalar multiple of the identity I. Define the sets

$$T = \{1 + e(m-1) \mid 1 \leq m \leq \ell\} \quad \text{and} \quad S = \{1, 2. \ldots, d\} \backslash T.$$

Let $y = (y_{ij}) \in C_{\mathfrak{gl}}(x)$ be some element in the centraliser of x, then by using Lemma 5.6.10 we find that $y_{i1} = 0$ for all $i \in S$, $y_{i-1,i} = 0$ for all $1 \neq i \in T$, $y_{ii} = y_{i+1,i+1}$ for all $i \in T$ and in case $e \geq 3$ we also find $y_{i,i+1} = y_{i+1,i+2}$ for all $i \in T$. Consequently, for $i \in S$ we have

$$\mathrm{Tr}(ye_{1i}) = 0$$

and hence, since y was an arbitrary element of $C_{\mathfrak{gl}}(x)$, we get that $e_{1i} \in C_{\mathfrak{gl}}(x)^{\perp}$ for all $i \in S$. Analogously we find $e_{i,i-1} \in C_{\mathfrak{gl}}(x)^{\perp}$ for $1 \neq i \in T$. Moreover, for $i \in T$ we compute

$$\mathrm{Tr}((e_{ii} - e_{i+1,i+1})y) = y_{ii} - y_{i+1,i+1} = 0$$

and hence $e_{ii} - e_{i+1,i+1} \in C_{\mathfrak{gl}}(x)^{\perp}$, since $y \in C_{\mathfrak{gl}}(x)^{\perp}$ was arbitrary. When $e \geq 3$ we find in a similar way that $e_{i+1,i} - e_{i+2,i+1} \in C_{\mathfrak{gl}}(x)^{\perp}$ for all $i \in T$.

Let $z = (z_{ij}) \in C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^{\perp})$ be some element. Because $e_{1i} \in C_{\mathfrak{gl}}(x)^{\perp}$ for $i \in S$, the element z satisfies $z_{11} = z_{ii}$ for all $i \in S$ and for each $i \in S$ all entries, except for the entry on the diagonal, in row i of z are zero. Because $e_{i,i-1} \in C_{\mathfrak{gl}}(x)^{\perp}$ for $1 \neq i \in T$, the element z satisfies $z_{ii} = z_{i-1,i-1}$ for all $1 \neq i \in T$. Since $e > 1$ we have $i - 1 \in S$ if $1 \neq i \in T$, it follows that all entries on the diagonal of z are equal.

Because $e_{ii} - e_{i+1,i+1} \in C_{\mathfrak{gl}}(x)^{\perp}$ for $i \in T$, we have in case char $k \neq 2$ that all entries in row i of z, except for the entry on the diagonal, are zero for all $i \in T$. This proves that z is a multiple of the identity matrix in case char $k \neq 2$. If char $k = 2$, then $e_{ii} - e_{i+1,i+1} \in C_{\mathfrak{gl}}(x)^{\perp}$ shows that for any $i \in T$ we have $z_{ij} = 0$ with $j \notin \{i, i+1\}$.

Assume $e \geq 3$, we will show that $z_{i,i+1} = 0$ for all $i \in T$. We showed above that $e_{i+1,i} - e_{i+2,i+1} \in C_{\mathfrak{gl}}(x)^{\perp}$ for all $i \in T$, so z satisfies the equation

$$(e_{i+1,i} - e_{i+2,i+1})z = z(e_{i+1,i} - e_{i+2,i+1})$$

for $i \in T$. Looking at the (i,i)-th entry on both sides of this equation, we see that $0 = z_{i,i+1}$ holds for $i \in T$. This proves that z is a multiple of the identity matrix.

In case char $k = 2$ and $e = 2$ it remains to show, that we have $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^\perp) \neq k \cdot I$, but $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^\perp)^\perp) = k \cdot I$. We will do this with an explicit calculation. Recall that ℓ is the number of Jordan blocks of size 2 and write $m \geq 0$ for the number of Jordan blocks of size 1. We then have $2\ell + m = d$ and hence m is odd, because $2 = \operatorname{char} k \nmid d$. If λ is the single eigenvalue of x, then the assumption $e = 2$ is equivalent to $(x - \lambda I)^2 = 0$. Without loss of generality we may assume that zero is the only eigenvalue of x. Write $J = \left(\begin{smallmatrix} 0 & 1 \\ 0 & \end{smallmatrix}\right)$ and $C(J) = \{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \mid a, b \in k\}$, so $x = \operatorname{diag}(J, \ldots, J, 0, \ldots, 0) \in \mathfrak{gl}_d(k)$ (with J, 0 appearing ℓ, respectively m times). The centraliser $C_{\mathfrak{gl}}(x)$ is given by

$$C_{\mathfrak{gl}}(x) = \left(\begin{array}{c|c|c|c} C(J) & \ldots & C(J) & \begin{smallmatrix} *_{1m} \\ 0_{1m} \end{smallmatrix} \\ \hline \vdots & \ddots & \vdots & \vdots \\ \hline C(J) & \ldots & C(J) & \begin{smallmatrix} *_{1m} \\ 0_{1m} \end{smallmatrix} \\ \hline 0_{m1}\ *_{m1} & \ldots & 0_{m1}\ *_{m1} & *_{mm} \end{array}\right)$$

with 0_{ij} denoting the zero matrix in $*_{ij} = \operatorname{Mat}_{ij}(k)$ ($*_{11} = *$). Computing $C_{\mathfrak{gl}}(x)^\perp$ gives

$$C_{\mathfrak{gl}}(x)^\perp = \left(\begin{array}{c|c|c|c} C(J) & \ldots & C(J) & \begin{smallmatrix} *_{1m} \\ 0_{1m} \end{smallmatrix} \\ \hline \vdots & \ddots & \vdots & \vdots \\ \hline C(J) & \ldots & C(J) & \begin{smallmatrix} *_{1m} \\ 0_{1m} \end{smallmatrix} \\ \hline 0_{m1}\ *_{m1} & \ldots & 0_{m1}\ *_{m1} & 0_{mm} \end{array}\right)$$

and with a bit of effort, we find that $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^\perp)$ is given by

$$C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^\perp) = k \cdot I \oplus k \cdot x$$

From here onward it is a straightforward computation to see that $C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(C_{\mathfrak{gl}}(x)^\perp)^\perp) = k \cdot I$. We can also do this without an explicit computation. Note that $d > 2$, since $e = 2$ and $2 \nmid d$. Write $V = k \cdot I \oplus k \cdot x$, then $\dim V = 2$ and hence $\dim V^\perp = \dim \mathfrak{gl}_d(k) - \dim V = d^2 - 2$. Because $d^2 - 2 > (d-1)^2 + 1$ for $d > 2$ we have $V^\perp \subsetneq C_{\mathfrak{gl}}(w)$ for all $w \in \mathfrak{gl}_d(k)$ not a multiple of the identity. This implies that $C_{\mathfrak{gl}}(V^\perp) = k \cdot I$.

□

Example 5.6.13. Let k be a field and for some $\lambda \in k$ let $x \in \mathfrak{gl}_9(k)$ be the matrix

$$x = \left(\begin{array}{ccc|ccc|cc|c} \lambda & 1 & & & & & & & \\ & \lambda & 1 & & & & & & \\ & & \lambda & & & & & & \\ \hline & & & \lambda & 1 & & & & \\ & & & & \lambda & 1 & & & \\ & & & & & \lambda & & & \\ \hline & & & & & & \lambda & 1 & \\ & & & & & & & \lambda & \\ \hline & & & & & & & & \lambda \end{array}\right).$$

The centraliser $C_{\mathfrak{gl}}(x)$ is given by all matrices in $\mathfrak{gl}_9(k)$ of the form

$$\left(\begin{array}{ccc|ccc|ccc} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 \\ & c_1 & c_2 & & c_4 & c_5 & & c_7 & \\ & & c_1 & & & c_4 & & & \\ \hline c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & c_{16} & c_{17} & c_{18} \\ & c_{10} & c_{11} & & c_{13} & c_{14} & & c_{16} & \\ & & c_{10} & & & c_{13} & & & \\ \hline & c_{19} & c_{20} & & c_{21} & c_{22} & c_{23} & c_{24} & c_{25} \\ & & c_{19} & & & c_{21} & & c_{23} & \\ \hline & & c_{26} & & & c_{27} & & c_{28} & c_{29} \end{array}\right)$$

with $c_i \in k$ and all other entries are zero. Consequently, $C_{\mathfrak{gl}}(x)^{\perp}$ is consists of all matrices in $\mathfrak{gl}_9(k)$ of the form

$$\left(\begin{array}{ccc|ccc|ccc} a_0 & * & * & a_3 & * & * & * & * & * \\ b_1 & a_1 & * & b_2 & a_4 & * & b_3 & * & * \\ 0 & -b_1 & a_2 & 0 & -b_2 & a_5 & 0 & -b_3 & 0 \\ \hline a_6 & * & * & a_9 & * & * & * & * & * \\ b_4 & a_7 & * & b_5 & a_{10} & * & b_6 & * & * \\ 0 & -b_4 & a_8 & 0 & -b_5 & a_{11} & 0 & -b_6 & 0 \\ \hline b_7 & * & * & b_8 & * & * & b_9 & * & * \\ 0 & -b_7 & * & 0 & -b_8 & * & 0 & -b_9 & 0 \\ \hline 0 & * & * & 0 & * & * & 0 & * & 0 \end{array}\right)$$

with $a_i, b_j \in k$ satisfying $a_{3k} + a_{1+3k} + a_{2+3k} = 0$ for $k \in \{0, 1, 2, 3\}$ and a "$*$" means that that entry can be chosen independently of all other entries.

5.6.2 On subspaces of $\mathfrak{sl}_3(k)$ containing no regular elements

Theorem 5.6.4 has the following important corollary.

Corollary 5.6.14. *Let $\mathbf{F}_q$ be the finite field of cardinality q with* char $\mathbf{F}_q \notin \{2, 3\}$. *There are $\binom{3}{1}_q^2 = (q^2+q+1)^2$ 1-dimensional toxic subspaces of $\mathfrak{sl}_3(\mathbf{F}_q)$.*

Proof. Write φ for the map $\mathfrak{gl}_3(\mathbf{F}_q) \to \mathfrak{sl}_3(\mathbf{F}_q) : x \mapsto x - \frac{\mathrm{Tr}(x)}{3} I$. For a 1-dimensional toxic subspace V of $\mathfrak{sl}_3(\mathbf{F}_q)$ there exists by Theorem 5.6.4 a unique pair of 1-dimensional subspaces $U, W \subseteq \mathbf{F}_q^3$ such that

$$V = \varphi(UW^T).$$

The number of 1-dimensional subspaces of $\mathbf{F}_q^3$ equals $\binom{3}{1}_q = q^2 + q + 1$ and hence the statement of the corollary follows. □

5.6.3 On subspaces of $\mathfrak{sl}_3(k)$ containing a regular element

Let k be a field with char $k \notin \{2,3\}$. We continue with our analysis of the behaviour of the map $V \mapsto [\mathfrak{sl}_3(k), V]$ for non-zero subspaces $V \subseteq \mathfrak{sl}_3(k)$. Theorem 5.6.4 covers the non-zero subspaces of $\mathfrak{sl}_3(k)$ having no regular elements (i.e. all elements are toxic). We therefore switch our attention to the case of subspaces of $\mathfrak{sl}_3(k)$ containig a regular element.

Lemma 5.6.15. *Let k be a field with* char $k \notin \{2,3\}$ *and let $V \subseteq \mathfrak{sl}_3(k)$ be a subspace with* $\dim V \geq 2$ *and containing a regular element. We have*

$$\dim [\mathfrak{sl}_3(k), V] = 6$$

if and only if $V = C_{\mathfrak{sl}}(x)$ for some regular element $x \in \mathfrak{sl}_3(k)$ (and hence $\dim V = 2$*).*

Proof. Suppose first that $\dim [\mathfrak{sl}_3(k), V] = 6$, then by Lemma 5.4.2 we have

$$\dim C_{\mathfrak{sl}}(V) = \dim \mathfrak{sl}_3(k) - \dim [\mathfrak{sl}_3(k), V] = 8 - 6 = 2.$$

Let $x \in V$ be regular (i.e. $\dim C_{\mathfrak{sl}}(x) = 2$). Then $C_{\mathfrak{sl}}(V) \subseteq C_{\mathfrak{sl}}(x)$ implies $C_{\mathfrak{sl}}(V) = C_{\mathfrak{sl}}(x)$. It follows that x commutes with every element of V, so $V \subseteq C_{\mathfrak{sl}}(x)$ and since $\dim V \geq 2$ we find that $V = C_{\mathfrak{sl}}(x)$, so in fact this forces $\dim V = 2$. For the other direction assume that $V = C_{\mathfrak{sl}}(x)$ for some regular element $x \in \mathfrak{sl}_3(k)$. Recall from Theorem 5.4.4 that $C_{\mathfrak{sl}}(C_{\mathfrak{sl}}(x)) = k[x] \cap \mathfrak{sl}_3(k)$ is two-dimensional. Together with Lemma 5.4.2 we find

$$\begin{aligned} \dim [\mathfrak{sl}_3(k), V] &= \dim C_{\mathfrak{sl}}(V)^{\perp} = \dim C_{\mathfrak{sl}}(C_{\mathfrak{sl}}(x))^{\perp} \\ &= \dim \mathfrak{sl}_3(k) - \dim C_{\mathfrak{sl}}(C_{\mathfrak{sl}}(x)) = 8 - 2 = 6. \end{aligned}$$

□

Lemma 5.6.16. *Let k be a field with* char $k \notin \{2,3\}$ *and let $V \subseteq \mathfrak{sl}_3(k)$ be subspace with* $\dim V \geq 3$*. We have* $\dim [\mathfrak{sl}_3(k), V] \in \{7,8\}$.

Proof. If V does not contain a regular element, then by Theorem 5.6.4 we have that $\dim V = 3$ and $\dim [\mathfrak{sl}_3(k), V] = 8$. When V contains a regular element, $x \in \mathfrak{sl}_3(k)$ say, then clearly $[\mathfrak{sl}_3(k), x] \subseteq [\mathfrak{sl}_3(k), V]$. Because x is regular we have $\dim[\mathfrak{sl}_3(k), x] = 6$ by Lemma 5.4.2 and hence $\dim [\mathfrak{sl}_3(k), V] \geq 6$. Equality cannot hold by Lemma 5.6.15, because $\dim V = 3$. It follows that $\dim[\mathfrak{sl}_3(k), V] \geq 7$. □

Lemma 5.6.17. *Let k be a field with* char $k \notin \{2,3\}$ *and let $V \subseteq \mathfrak{sl}_3(k)$ be subspace with* $\dim [\mathfrak{sl}_3(k), V] = 7$*. Then we have $V \subseteq C_{\mathfrak{sl}}(U)$ for some unique one-dimensional toxic subspace $U \subseteq \mathfrak{sl}_3(k)$.*

In other words, up to multiplication by a non-zero scalar in k there exists a unique toxic element $x \in \mathfrak{sl}_3(k)$ with $V \subseteq C_{\mathfrak{sl}}(x)$.

Proof. By Lemma 5.4.8 there exists a non-zero element $x \in \mathfrak{sl}_3(k)$ with $V \subseteq C_{\mathfrak{sl}}(x)$. If x is regular, then $C_{\mathfrak{sl}}(x)$ is two dimensional. So V is one-dimensional, in which case $\dim[\mathfrak{sl}_3(k), V] \in \{4, 6\}$, or $V = C_{\mathfrak{sl}}(x)$, in which case $\dim[\mathfrak{sl}_3(k), V] = 6$ by Lemma 5.6.15. In either case we get a contradiction with the assumption $\dim[\mathfrak{sl}_3(k), V] = 7$, it follows that x must be toxic. Conversely, if $V \subseteq C_{\mathfrak{sl}}(U)$ for some unique one-dimensional toxic subspace $U = k \cdot x \subseteq \mathfrak{sl}_3(k)$, then this implies

$$k \cdot x = k[x] \cap \mathfrak{sl}_3(k) = C_{\mathfrak{sl}}(C_{\mathfrak{sl}}(x)) \subseteq C_{\mathfrak{sl}}(V),$$

using that x is toxic for the first equality and Theorem 5.4.4 for the second equality. From $\dim[\mathfrak{sl}_3(k), V] = 7$ it follows by Lemma 5.4.2 that $\dim C_{\mathfrak{sl}}(V) = 1$ and hence $C_{\mathfrak{sl}}(V) = k \cdot x = U$. □

5.6.4 Calculations in $\mathfrak{sl}_3(\mathbf{F}_q)$

We record here a few helpful results.

Lemma 5.6.18. *Let $\mathbf{F}_q$ be the finite field with q elements with* $\operatorname{char} \mathbf{F}_q \notin \{2, 3\}$. *The number of different subspaces of $\mathfrak{sl}_3(\mathbf{F}_q)$ of the form $C_{\mathfrak{sl}}(x)$ with $x \in \mathfrak{sl}_3(\mathbf{F}_q)$*

- *toxic and nilpotent is $(q^2 + q + 1)(q + 1)$;*
- *toxic and non-nilpotent is $(q^2 + q + 1)q^2$.*

Proof. Let $x, y \in \mathfrak{sl}_3(\mathbf{F}_q)$ be two toxic elements satisfying $C_{\mathfrak{sl}}(x) = C_{\mathfrak{sl}}(y)$. Using Theorem 5.4.4 we see that $\mathbf{F}_q[x] \cap \mathfrak{sl}_3(\mathbf{F}_q) = \mathbf{F}_q[y] \cap \mathfrak{sl}_3(\mathbf{F}_q)$. From the (proof of) Lemma 5.4.12 we see that the minimal polynomials of x and y have degree 2. It follows that x and y span the same subspace of $\mathfrak{sl}_3(\mathbf{F}_q)$ because $I \notin \mathfrak{sl}_3(\mathbf{F}_q)$. This shows that

$$|\{C_{\mathfrak{sl}}(x) \mid x \in \mathfrak{sl}_3(\mathbf{F}_q) \text{ toxic and nilpotent}\}| = |\{\mathbf{F}_q \cdot x \mid x \in \mathfrak{sl}_3(\mathbf{F}_q) \text{ toxic and nilpotent}\}| \tag{5.32}$$

and similar for case of toxic and non-nilpotent.

By Lemma 5.4.12 any toxic and nilpotent element of $\mathfrak{sl}_3(\mathbf{F}_q)$ is $\mathrm{GL}_3(\mathbf{F}_q)$-conjugate to $n = \left(\begin{smallmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$. Hence the right-hand side of equation (5.32) times $q-1$ equals the size of the orbit of n under the conjugation action of $\mathrm{GL}_3(\mathbf{F}_q)$ on $\mathfrak{sl}_3(\mathbf{F}_q)$. The stabiliser of n under this action equals

$$\left\{ \left(\begin{smallmatrix} a & b & c \\ & d & e \\ & & a \end{smallmatrix}\right) \mid a, d \in \mathbf{F}_q^* \text{ and } b, c, e \in \mathbf{F}_q \right\}.$$

By the orbit stabiliser theorem we can compute the size of the orbit of n under $\mathrm{GL}_3(\mathbf{F}_q)$, it is equal to

$$\frac{|\mathrm{GL}_3(\mathbf{F}_q)|}{(q-1)^2 q^3} = (q^2 + q + 1)(q^2 - 1)$$

and hence there are $(q^2+q+1)(q+1)$ subspaces of the form $C_{\mathfrak{sl}}(x)$ with x toxic and nilpotent.

If $x \in \mathfrak{sl}_3(\mathbf{F}_q)$ is toxic and non-nilpotent, then by Lemma 5.4.12 the element x is $\mathrm{GL}_3(\mathbf{F}_q)$-conjugate to $\lambda n'$ for some unique $\lambda \in \mathbf{F}_q^*$, where $n' = \left(\begin{smallmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$. It follows that

$$|\{C_{\mathfrak{sl}}(x) \mid x \in \mathfrak{sl}_3(\mathbf{F}_q) \text{ toxic and non-nilpotent}\}|$$

equals the size of the orbit of n' under the conjugation action of $\mathrm{GL}_3(\mathbf{F}_q)$ on $\mathfrak{sl}_3(\mathbf{F}_q)$. The stabliser of n' under this action equals

$$\begin{pmatrix} \mathbf{F}_q^* & \\ & \mathrm{GL}_2(\mathbf{F}_q) \end{pmatrix}.$$

Using the orbit stabiliser theorem, we conclude that there are

$$\frac{|\mathrm{GL}_3(\mathbf{F}_q)|}{(q-1)|\mathrm{GL}_2(\mathbf{F}_q)|} = (q^2+q+1)q^2$$

subspaces of the form $C_{\mathfrak{sl}}(x)$ with x toxic and non-nilpotent. □

Remark 5.6.19. As a sanity check the lemma shows that there are $(q^2+q+1)^2$ subspaces in $\mathfrak{sl}_3(\mathbf{F}_q)$ of the form $C_{\mathfrak{sl}}(x)$ with x toxic. This is also the conclusion of Corollary 5.6.14.

Lemma 5.6.20. *Let $\mathbf{F}_q$ be the finite field with q elements and satisfying* $\mathrm{char}\ \mathbf{F}_q \neq 3$. *The number of elements in $\mathfrak{sl}_3(\mathbf{F}_q)$ of type 1 to 5 is displayed in Table 5.3. The number of one-dimensional subspaces of $\mathfrak{sl}_3(\mathbf{F}_q)$ containing an element of a certain type, can be obtained by dividing the corresponding entry in Table 5.3 by $q-1$.*

Type	$\lvert\mathfrak{sl}_3(\mathbf{F}_q) \cap \{\text{Type}\}\rvert$
1	$q^8-q^7-q^6+q^4$
2	$q^2(q^3-1)(q^2-1)$
3	$(q^3-1)(q^3-q)$
4	$(q^3-1)(q+1)$
5	$q^2(q^3-1)$

Table 5.3: Number of elements in $\mathfrak{sl}_3(\mathbf{F}_q)$ of each type.

Proof. Let $x \in \mathfrak{sl}_3(\mathbf{F}_q)$ be an element of type 2, 3, 4 or 5. Then all eigenvalues of x are in $\mathbf{F}_q$. So x is conjugate, by an element of $G = \mathrm{GL}_3(\mathbf{F}_q)$, to the Jordan normal form displayed in Table 5.1. The group $\mathrm{GL}_3(\mathbf{F}_q)$ acts through conjugation on $\mathfrak{sl}_3(\mathbf{F}_q)$ and hence the number of elements in $\mathfrak{sl}_3(\mathbf{F}_q)$ with a fixed Jordan normal form z from Table 5.1 equals the size of the orbit $\mathrm{Orb}_G(z)$ of z under this action. By the orbit stabiliser theorem the size of this orbit equals the index of the stabiliser $\mathrm{Stab}_G(z)$ of z in $\mathrm{GL}_3(\mathbf{F}_q)$. Compare to this table to [2, Ap. B]. This gives us a recipe to compute the size of the orbit. We consider the cases of type 2, 3, 4 and 5 separately.

- Type 2. Fix $\lambda \in \mathbf{F}_q^*$, then our element z is given by

$$z = \begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & -2\lambda \end{pmatrix} \quad \text{and} \quad \mathrm{Stab}_G(z) = \left\{ \begin{pmatrix} a & c & \\ & a & \\ & & b \end{pmatrix} \mid a, b \in \mathbf{F}_q^*, c \in \mathbf{F}_q \right\}$$

  with $-2\lambda \neq \lambda$ since char $\mathbf{F}_q \neq 3$. It follows that

$$|\mathrm{Orb}_G(z)| = \frac{|\mathrm{GL}_3(\mathbf{F}_q)|}{|\mathrm{Stab}_G(z)|} = \frac{(q^3-1)(q^3-q)(q^3-q^2)}{(q-1)^2 q} = q^2(q^3-1)(q+1)$$

  and consequently, since there are $q-1$ choices for λ, there are $q^2(q^3-1)(q^2-1)$ elements of type 2.

- Type 3. Since $z \in \mathfrak{sl}_3(\mathbf{F}_q)$ with char $\mathbf{F}_q \neq 3$ this forces $\lambda = 0$, so z is given by

$$z = \begin{pmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{pmatrix} \quad \text{and} \quad \mathrm{Stab}_G(z) = \left\{ \begin{pmatrix} a & b & c \\ & a & b \\ & & a \end{pmatrix} \mid a \in \mathbf{F}_q^*, b, c \in \mathbf{F}_q \right\}.$$

  It follows that

$$|\mathrm{Orb}_G(z)| = \frac{|\mathrm{GL}_3(\mathbf{F}_q)|}{|\mathrm{Stab}_G(z)|} = \frac{(q^3-1)(q^3-q)(q^3-q^2)}{(q-1)q^2} = (q^3-1)(q^3-q)$$

  and hence there are $(q^3-1)(q^3-q)$ elements of type 3.

- Type 4. Since $z \in \mathfrak{sl}_3(\mathbf{F}_q)$ with char $\mathbf{F}_q \neq 3$ this forces $\lambda = 0$, so z is given by

$$z = \begin{pmatrix} 0 & 0 & 1 \\ & 0 & 0 \\ & & 0 \end{pmatrix} \quad \text{and} \quad \mathrm{Stab}_G(z) = \left\{ \begin{pmatrix} a & c & e \\ b & d & \\ & a & \end{pmatrix} \mid a, b \in \mathbf{F}_q^*, c, d, e \in \mathbf{F}_q \right\}.$$

  It follows that

$$|\mathrm{Orb}_G(z)| = \frac{|\mathrm{GL}_3(\mathbf{F}_q)|}{|\mathrm{Stab}_G(z)|} = \frac{(q^3-1)(q^3-q)(q^3-q^2)}{(q-1)^2 q^3} = (q^3-1)(q+1)$$

  and hence there are $(q^3-1)(q+1)$ elements of type 4.

- Type 5. Fix $\lambda \in \mathbf{F}_q^*$, then our element z is given by

$$z = \begin{pmatrix} \lambda & & \\ & \lambda & \\ & & -2\lambda \end{pmatrix} \quad \text{and} \quad \mathrm{Stab}_G(z) = \begin{pmatrix} \mathrm{GL}_2(\mathbf{F}_q) & \\ & \mathbf{F}_q^* \end{pmatrix}$$

  with $-2\lambda \neq \lambda$ since char $\mathbf{F}_q \neq 3$. It follows that

$$|\mathrm{Orb}_G(z)| = \frac{|\mathrm{GL}_3(\mathbf{F}_q)|}{|\mathrm{Stab}_G(z)|} = \frac{(q^3-1)(q^3-q)(q^3-q^2)}{(q^2-1)(q^2-q)(q-1)} = q^2(q^2+q+1)$$

  and consequently, since there are $q-1$ choices for λ, there are $q^2(q^3-1)$ elements of type 5.

The number of elements of type 1 is obtained as the difference between $q^8 - 1$ and the number of elements of type 2, 3, 4 and 5. □

Lemma 5.6.21. *Let k be a field with* char $k \notin \{2, 3\}$ *and $x \in \mathfrak{sl}_3(k)$ a non-zero element. We have $x \in [\mathfrak{sl}_3(k), x]$ if and only if x is of type 3 or 4.*

Proof. Assume $x \in [\mathfrak{sl}_3(k), x] = C_{\mathfrak{sl}}(x)^\perp$ then $B(x, C_{\mathfrak{sl}}(x)) = 0$ and because $x \in C_{\mathfrak{sl}}(x)$ we get $\mathrm{Tr}(x^2) = B(x, x) = 0$. This is already enough to rule out some types. For type 2 and 5 the eigenvalues of x are λ (multiplicity 2) and -2λ for some $\lambda \in k^*$. So $\mathrm{Tr}(x^2) = \lambda^2 + \lambda^2 + (-2\lambda)^2 = 6\lambda^2$, which is non-zero because $\lambda \neq 0$ and char $k \notin \{2, 3\}$. Hence x is not of type 2 or 5. Next we show that x is not of type 1 either. Without loss of generality we may assume that k is algebraically closed. Let x be an element of type 1 and after conjugation we may assume that x is in diagonal form, then by Lemma 5.4.2

$$[\mathfrak{sl}_3(k), x] = C_{\mathfrak{sl}}(x)^\perp = \begin{pmatrix} * & & \\ & * & \\ & & * \end{pmatrix}^\perp = \begin{pmatrix} 0 & * & * \\ * & 0 & * \\ * & * & 0 \end{pmatrix}$$

and hence $x \notin [\mathfrak{sl}_3(k), x]$. Finally, we will show that if $x \in \mathfrak{sl}_3(k)$ is of type 3 or 4, then we do have $x \in [\mathfrak{sl}_3(k), x]$. Without loss of generality we may assume that x is in Jordan normal form. So if x is of type 3, then $x = \begin{pmatrix} 0 & 1 & \\ & 0 & 1 \\ & & 0 \end{pmatrix}$ and hence by Lemma 5.4.2 we have

$$[\mathfrak{sl}_3(k), x] = C_{\mathfrak{sl}}(x)^\perp = \left\{ \begin{pmatrix} 0 & a & b \\ & 0 & a \\ & & 0 \end{pmatrix} \mid a, b \in k \right\}^\perp = \left\{ \begin{pmatrix} * & * & * \\ a & * & * \\ 0 & -a & * \end{pmatrix} \mid a \in k \right\} \cap \mathfrak{sl}_3(k).$$

Clearly in this case we have $x \in [\mathfrak{sl}_3(k), x]$. If x is of type 4, then we only need to consider $x = \begin{pmatrix} 0 & 0 & 1 \\ & 0 & \\ & & 0 \end{pmatrix}$ and hence by Lemma 5.4.2 we have

$$[\mathfrak{sl}_3(k), x] = C_{\mathfrak{sl}}(x)^\perp = \left\{ \begin{pmatrix} a & * & * \\ & -2a & * \\ & & a \end{pmatrix} \mid a \in k \right\}^\perp = \left\{ \begin{pmatrix} a & * & * \\ & * & \\ & & -a \end{pmatrix} \mid a \in k \right\} \cap \mathfrak{sl}_3(k),$$

using that char $k \nmid 3$. Again it is clear that $x \in [\mathfrak{sl}_3(k), x]$. □

The case $\dim V = 1$

For $\delta_K \in \{0, 1\}$ and one-dimensional subspaces $V \subseteq \mathfrak{sl}_d(\mathbf{F}_q)$ we investigate the map

$$V \mapsto \delta_K V + [\mathfrak{sl}_3(\mathbf{F}_q), V].$$

Lemma 5.6.22. *Let $\mathbf{F}_q$ be the finite field of cardinality q with* char $\mathbf{F}_q \notin \{2, 3\}$. *Let $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ be a one-dimensional subspace.*

(a) We then have

$$\dim [\mathfrak{sl}_3(\mathbf{F}_q), V] \in \{4, 6\} \quad \text{and} \quad \dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] \in \{4, 5, 6, 7\}.$$

(b) Write $\ell = \dim [\mathfrak{sl}_3(\mathbf{F}_q), V]$*, then if*

- $\ell = 4$*, we have* $(q^2+q+1)^2$ *such subspaces* V*;*
- $\ell = 6$*, we have* $\binom{8}{1}_q - (q^2+q+1)^2$ *such subspaces* V*.*

(c) Write $\ell = \dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V]$*. Then if*

- $\ell = 4$*, we have* $(q^2+q+1)(q+1)$ *such subspaces* V*;*
- $\ell = 5$*, we have* $(q^2+q+1)q^2$ *such subspaces* V*;*
- $\ell = 6$*, we have* $(q^3-1)(q^2+q)$ *such subspaces* V*;*
- $\ell = 7$*, we have* $q^7+q^6-q^4-q^3-q^2$ *such subspaces* V*.*

Proof. Let $x \in \mathfrak{sl}_3(\mathbf{F}_q)$ be a non-zero element and write $V = \mathbf{F}_q \cdot x$ for the subspace spanned by x. Recall that $\dim C_{\mathfrak{sl}}(x)$ equals 2 or 4 if and only if x is regular, respectively toxic. From Lemma 5.4.2 it follows that

$$\dim [\mathfrak{sl}_3(\mathbf{F}_q), x] = \dim\, C_{\mathfrak{sl}}(x)^{\perp} = 8 - \dim C_{\mathfrak{sl}}(x)$$

and hence $\dim [\mathfrak{sl}_3(\mathbf{F}_q), V]$ equals 6, respectively 4 if and only if V contains a regular, respectively toxic element. If follows from Lemma 5.6.20 that there are $(q^2+q+1)^2$, respectively $\binom{8}{1}_q - (q^2+q+1)^2$ one-dimensional toxic, respectively regular, subspaces of $\mathfrak{sl}_3(\mathbf{F}_q)$. Note that the number of one-dimensional subspaces of $\mathfrak{sl}_3(\mathbf{F}_q)$ equals $\binom{8}{1}_q$, see also Chapter 2.

Because V is one-dimensional, we have

$$\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 1 + \dim [\mathfrak{sl}_3(\mathbf{F}_q), V]$$

if $V \not\subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$ and

$$\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = \dim [\mathfrak{sl}_3(\mathbf{F}_q), V]$$

if $V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$. We know from Lemma 5.6.21 that $V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$ if and only if x is of type 3 or 4. Combining the above with Table 5.3 and the fact that x is regular if and only x is of type 1, 2 or 3, implies part (c). In particular $\ell = 4$ if x is of type 4, $\ell = 5$ if x is of type 5, $\ell = 6$ if x is of type 3 and $\ell = 7$ if x is of type 1 or 2. □

The case $\dim V = 2$

For $\delta_K \in \{0, 1\}$ and two-dimensional subspaces $V \subseteq \mathfrak{sl}_d(\mathbf{F}_q)$ we investigate the map

$$V \mapsto \delta_K V + [\mathfrak{sl}_3(\mathbf{F}_q), V].$$

The first lemma deals with the case of a two-dimensional toxic subspace.

Lemma 5.6.23. *Let $\mathbf{F}_q$ be the finite field of cardinality q with $\operatorname{char}\mathbf{F}_q \notin \{2,3\}$. Let $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ be a two-dimensional toxic subspace.*

(a) We then have

$$\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 6 \quad \text{and} \quad \dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] \in \{6,7\}.$$

(b) There are $2(q^2+q+1)^2$ such subspaces V with $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 6$.

(c) Write $\ell = \dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V]$, then if

- *$\ell = 6$, we have $2(q^2+q+1)$ such subspaces V;*
- *$\ell = 7$, we have $2(q^2+q+1)(q^2+q)$ such subspaces V.*

Proof. The first statement of part (a) follows immediately from Theorem 5.6.4. The same theorem also shows that $V = \varphi(UW^T)$ or $V = \varphi(WU^T)$ for unique subspaces $U, W \subseteq \mathbf{F}_q^3$ with $\dim U = 2$, $\dim W = 1$; here φ is the map $\mathfrak{gl}_3(\mathbf{F}_q) \to \mathfrak{sl}_3(\mathbf{F}_q), x \mapsto x - \frac{\operatorname{Tr}(x)}{3} I$. There are $\binom{3}{2}_q = \binom{3}{1}_q = q^2+q+1$ choices for U and W, it follows that there are $2(q^2+q+1)^2$ two-dimensional toxic subspaces V satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 6$.

Without loss of generality we may assume that $V = \varphi(UW^T)$ and, after conjugating with a suitable element $g \in \mathrm{GL}_3(\mathbf{F}_q)$ satisfying $gU = \langle e_1, e_2\rangle$, we may further assume that $U = \langle e_1, e_2\rangle = \mathbf{F}_q \cdot e_1 \oplus \mathbf{F}_q \cdot e_2$. Write $W = \mathbf{F}_q \cdot x$ for some $0 \neq x = (x_1, x_2, x_3)^T \in \mathbf{F}_q^3$, then V is given by

$$V = \mathbf{F}_q \cdot \begin{pmatrix} 2x_1 & 3x_2 & 3x_3 \\ 0 & -x_1 & 0 \\ 0 & 0 & -x_1 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} -x_2 & 0 & 0 \\ 3x_1 & 2x_2 & 3x_3 \\ 0 & 0 & -x_2 \end{pmatrix}. \tag{5.33}$$

By calculating the bracket $[y, z]$ explicitly for all basis elements $y \in \mathfrak{sl}_3(\mathbf{F}_q)$ and the two matrices in (5.33), we see that $[\mathfrak{sl}_3(\mathbf{F}_q), V]$ is given by

$$[\mathfrak{sl}_3(\mathbf{F}_q), V] = \begin{pmatrix} 0 & * & * \\ * & 0 & * \\ 0 & 0 & 0 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} -x_3 & 0 & 0 \\ 0 & 0 & 0 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

and hence that

$$V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = \begin{pmatrix} 0 & * & * \\ * & 0 & * \\ 0 & 0 & 0 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} -x_3 & 0 & 0 \\ 0 & 0 & 0 \\ x_1 & x_2 & x_3 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & x_1 & 0 \\ 0 & 0 & -x_1 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & x_2 & 0 \\ 0 & 0 & -x_2 \end{pmatrix}.$$

It follows that

$$\left(V + [\mathfrak{sl}_3(\mathbf{F}_q), V]\right) / [\mathfrak{sl}_3(\mathbf{F}_q), V] \cong \mathbf{F}_q \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & x_1 & 0 \\ 0 & 0 & -x_1 \end{pmatrix} + \mathbf{F}_q \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & x_2 & 0 \\ 0 & 0 & -x_2 \end{pmatrix}$$

and hence we have $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 6$ if $x_1 = x_2 = 0$ and $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$ otherwise.

The above computation shows, after fixing a two-dimensional space $U \subseteq \mathbf{F}_q^3$, that there exists a unique one-dimensional space $W \subseteq \mathbf{F}_q^3$ for which the two-dimensional toxic

subspace $V = \varphi(UW^T)$ satisfies $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 6$. A similar statement holds for $V = \varphi(WU^T)$. There are $\binom{3}{2}_q = q^2 + q + 1$ choices for a subspace $U \subseteq \mathbf{F}_q^3$, hence there are $2(q^2+q+1)$ two-dimensional toxic subspaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ satisfying $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$. Consequently, there are $2(q^2+q+1)(q^2+q)$ two-dimensional toxic subspaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ satisfying $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 6$. □

Lemma 5.6.24. *Let $\mathbf{F}_q$ be the finite field of cardinality q with $\operatorname{char} \mathbf{F}_q \notin \{2, 3\}$. Let $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ be a two-dimensional subspace containing a regular element and satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 6$. Then $V = C_{\mathfrak{sl}}(x)$ for some regular $x \in \mathfrak{sl}_3(\mathbf{F}_q)$ (i.e. x is of type 1, 2 or 3).*

(a) If x is of type

- *1a, then there are $\frac{1}{6}(q^2+q+1)(q+1)q^3$ such subspaces V;*
- *1b, then there are $\frac{1}{2}(q^3-1)q^3$ such subspaces V;*
- *1c, then there are $\frac{1}{3}(q+1)(q-1)^2q^3$ such subspaces V;*
- *2, then there are $(q^2+q+1)(q+1)q^2$ such subspaces V;*
- *3, then there are $(q^3-1)(q+1)$ such subspaces V;*

(b) Write $\ell = \dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V]$; then if x is of type

- *3, then $\ell = 6$ and we have $(q^3-1)(q+1)$ such subspaces V;*
- *2, then $\ell = 7$ and we have $(q^2+q+1)(q+1)q^2$ such subspaces V;*
- *1, then $\ell = 8$.*

Proof. That V is of the form $C_{\mathfrak{sl}}(x)$ for some regular $x \in \mathfrak{sl}_3(\mathbf{F}_q)$ is the statement of Lemma 5.6.15. Suppose x has type i, then x gives rise to the centraliser $C_{\mathfrak{sl}}(x)$. Of course, there are other elements of type i giving rise to the same centraliser $C_{\mathfrak{sl}}(x)$. For each i this number is recorded in Table 5.2. So dividing the total number of elements in $\mathfrak{sl}_3(\mathbf{F}_q)$ of type i by the corresponding entry in Table 5.2 gives the total number of spaces of the form $C_{\mathfrak{sl}}(x)$ with x of type i. Table 5.4 lists for each type the number of orbits under the conjugation action of $\mathrm{GL}_3(\mathbf{F}_q)$ on $\mathfrak{sl}_3(\mathbf{F}_q)$ and the size of each orbit. This table is Table 7.1 in [2]. The content of this table can also be derived by the theory established in this chapter. Doing this explicitly results in part (a).

For part (b) we only need to show that, when x is of type 3, 2 or 1, that ℓ equals 6, 7 or 8 respectively. The rest follows from part (a). Suppose x is of type 3, then without loss of generality $x = \left(\begin{smallmatrix} 0 & 1 & \\ 0 & 1 & \\ & & 0 \end{smallmatrix}\right)$ and hence

$$\left\{\left(\begin{smallmatrix} 0 & a & b \\ 0 & a & \\ & & 0 \end{smallmatrix}\right) \mid a, b \in k\right\} = C_{\mathfrak{sl}}(x) \subseteq [\mathfrak{sl}_3(k), C_{\mathfrak{sl}}(x)] = (\mathbf{F}_q \cdot x)^\perp = \left\{\left(\begin{smallmatrix} * & * & * \\ a & * & * \\ 0 & -a & * \end{smallmatrix}\right) \mid a \in k\right\} \cap \mathfrak{sl}_3(k).$$

This shows that for $V = C_{\mathfrak{sl}}(x)$ with x of type 3, we have $V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$. Suppose next that x is of type 2, then without loss of generality $x = \left(\begin{smallmatrix} \lambda & 1 & \\ & \lambda & \\ & & -2\lambda \end{smallmatrix}\right)$ for some $\lambda \in \mathbf{F}_q$. We then have

$$C_{\mathfrak{sl}}(x) = \mathbf{F}_q \cdot \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) + \mathbf{F}_q \cdot \left(\begin{smallmatrix} 1 & & \\ & 1 & \\ & & -2 \end{smallmatrix}\right)$$

and

$$[\mathfrak{sl}_3(\mathbf{F}_q), C_{\mathfrak{sl}}(x)] = \left(\begin{smallmatrix} * & * & * \\ 0 & * & * \\ * & * & * \end{smallmatrix}\right) \cap \left(\begin{smallmatrix} * & * & * \\ * & * & * \\ * & * & 0 \end{smallmatrix}\right) \cap \mathfrak{sl}_3(\mathbf{F}_q) = \left(\begin{smallmatrix} 0 & * & * \\ 0 & 0 & * \\ * & * & 0 \end{smallmatrix}\right) + \mathbf{F}_q \cdot \left(\begin{smallmatrix} 1 & & \\ & -1 & \\ & & 0 \end{smallmatrix}\right).$$

Writing $V = C_{\mathfrak{sl}}(x)$, it follows that

$$V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = \left(\begin{smallmatrix} * & * & * \\ 0 & * & * \\ * & * & * \end{smallmatrix}\right) \cap \mathfrak{sl}_3(\mathbf{F}_q),$$

which is 7 dimensional. Finally, assume x is of type 1. By extension of scalars we may work with $k = \overline{\mathbf{F}}_q$, an algebraic closure of $\mathbf{F}_q$, in order to compute the dimension of $V + [\mathfrak{sl}_3(\mathbf{F}_q), V]$. Over k, we can assume without loss of generality that x is diagonal, i.e. $x = \left(\begin{smallmatrix} \alpha & & \\ & \beta & \\ & & \gamma \end{smallmatrix}\right)$ with $\alpha, \beta, \gamma \in k$. In which case we have

$$C_{\mathfrak{sl}}(x) = \left(\begin{smallmatrix} * & & \\ & * & \\ & & * \end{smallmatrix}\right) \quad \text{and} \quad [\mathfrak{sl}_3(k), C_{\mathfrak{sl}}(x)] = \left(\begin{smallmatrix} 0 & * & * \\ * & 0 & * \\ * & * & 0 \end{smallmatrix}\right)$$

and hence, writing $V = C_{\mathfrak{sl}}(x)$, we have $\dim_k V + [\mathfrak{sl}_3(k), V] = 8$. It follows that we also have $\dim_{\mathbf{F}_q} V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 8$ □

Type	Number of orbits	Size of each orbit
1a	$\frac{1}{6}(q-1)(q-2)$	$(q^2+q+1)(q+1)q^3$
1b	$\frac{1}{2}(q-1)q$	$(q^3-1)q^3$
1c	$\frac{1}{3}(q^2-1)$	$(q+1)(q-1)^2q^3$
2	$q-1$	$(q^3-1)(q+1)q^2$
3	1	$(q^3-1)(q^2-1)q$
4	1	$(q^3-1)(q+1)$
5	$q-1$	$(q^2+q+1)q^2$

Table 5.4: Orbits in $\mathfrak{sl}_3(\mathbf{F}_q)$ under the conjugation action of $\mathrm{GL}_3(\mathbf{F}_q)$. This is Table 7.1 from [2].

Lemma 5.6.25. *Let $\mathbf{F}_q$ be the finite field of cardinality q with* char $\mathbf{F}_q \notin \{2, 3\}$. *There are*

$$\binom{4}{2}_q (q^2+q+1)^2 - (q^2+q+1)(q^4+4q^3+7q^2+4q+1)$$

two-dimensional subspaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ satisfying $\dim [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$.

Proof. Since $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$, we have by Lemma 5.6.17 that $V \subseteq C_{\mathfrak{sl}}(x)$ for some toxic $x \in \mathfrak{sl}_3(\mathbf{F}_q)$. On the other hand, if $V' \subseteq C_{\mathfrak{sl}}(x)$ is a two dimensional subspace, then $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] \in \{6, 7\}$. One can see this as follows, if V' is toxic, then by Theorem 5.6.4 we have $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = 6$, and if V' contains a regular element, then $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] \geq 6$, because the image of a regular element under taking the bracket with $\mathfrak{sl}_3(\mathbf{F}_q)$ is already six-dimensional. The inclusion $V \subseteq C_{\mathfrak{sl}}(x)$ implies that $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] \leq 7$. As Theorem 5.6.4 and Lemma 5.6.15 show, our understanding of two-dimensional subspaces $V' \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ with $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = 6$ is good. Therefore, we will calculate the number of two-dimensional subspaces $V' \subseteq C_{\mathfrak{sl}}(x)$, for some toxic $x \in \mathfrak{sl}_3(\mathbf{F}_q)$, satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = 6$. The number of two-dimensional subspaces $V \subseteq C_{\mathfrak{sl}}(x)$ with $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$ can then readily be computed, since the total number of two-dimensional subspaces of $C_{\mathfrak{sl}}(x)$ is $\binom{4}{2}_q$.

For our calculations we need to distinguish between the two possible types of x. Recall first the map $\varphi : \mathfrak{gl}_3(\mathbf{F}_q) \to \mathfrak{sl}_3(\mathbf{F}_q) : x \mapsto x - \frac{\mathrm{Tr}(x)}{3} I$. Assume x is of type 4, then without loss of generality $x = \left(\begin{smallmatrix} 0 & 0 & 1 \\ & 0 & \\ & & 0 \end{smallmatrix}\right)$. In this case we have

$$C_{\mathfrak{sl}}(x) = \left\{ \left(\begin{smallmatrix} a & * & * \\ 0 & -2a & * \\ 0 & 0 & a \end{smallmatrix}\right) \mid a \in \mathbf{F}_q \right\}. \tag{5.34}$$

Two-dimensional subspaces $V' \subseteq C_{\mathfrak{sl}}(x)$ with $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = 6$ come in two flavours: V' is a toxic subspace or V' contains a regular element. We start by calculating the number of two-dimensional toxic subspaces of $C_{\mathfrak{sl}}(x)$.

- Assume V' is a two-dimensional toxic subspace of $C_{\mathfrak{sl}}(x)$. By Theorem 5.6.4 we have $V' = \varphi(UW^T)$ or $V' = \varphi(WU^T)$ for unique subspaces $U, W \subseteq \mathbf{F}_q^3$ with $\dim U = 2$ and $\dim W = 1$. Without loss of generality we assume $V' = \varphi(UW^T)$, the calculation for the other case goes analogously and the end result is the same. Any toxic element in $C_{\mathfrak{sl}}(x)$ can be uniquely written as $\lambda I + y$ for some scalar $\lambda \in \mathbf{F}_q$ and some matrix $y \in \mathfrak{gl}_3(\mathbf{F}_q)$ of rank 1. From the explicit description in (5.34) we deduce that $\lambda = a$, since otherwise the rank of y will never equal 1. Using that $\mathrm{char}\, \mathbf{F}_q \neq 3$, this shows that
$$UW^T \subseteq \left(\begin{smallmatrix} 0 & * & * \\ 0 & * & * \\ 0 & 0 & 0 \end{smallmatrix}\right)$$
and hence forces $U = \langle e_1, e_2 \rangle$ and $W \subseteq \{0\} \oplus \mathbf{F}_q^2$. This gives $\binom{2}{1}_q = q + 1$ possibilities for W and all of them result in toxic two-dimensional subspaces of $C_{\mathfrak{sl}}(x)$. This shows that there are $2(q+1)$ possibilities for V'.

Next we calculate the number of subspaces of $C_{\mathfrak{sl}}(x)$ which are of the form $C_{\mathfrak{sl}}(z)$ for some regular $z \in \mathfrak{sl}_3(\mathbf{F}_q)$. By the description in (5.34) the eigenvalues of any element of $C_{\mathfrak{sl}}(x)$ lie in $\mathbf{F}_q$ and one eigenvalue occurs with multiplicity at least two. So any regular element $z \in C_{\mathfrak{sl}}(x)$ is of type 2 or 3. Note that, if $z \in C_{\mathfrak{sl}}(x)$ is regular, then $C_{\mathfrak{sl}}(z) = k[z] \subseteq C_{\mathfrak{sl}}(x)$.

- Suppose $z = \left(\begin{smallmatrix} a & b & d \\ 0 & -2a & c \\ 0 & 0 & a \end{smallmatrix}\right) \in C_{\mathfrak{sl}}(x)$ is a regular element of type 2. The eigenvalues of z are $a, -2a$ with $a \neq 0$ and the minimal polynomial of z is given by $(T-a)^2(T+2a) \in \mathbf{F}_q[T]$. We already know the eigenvalues of z with multiplicity, so we see that z being regular of type 2 is equivalent to $(z - aI)(z + 2aI)$ being non-zero. We compute

$$(z - aI)(z + 2aI) = \left(\begin{smallmatrix} 0 & 0 & 3ad+bc \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$$

  and hence z is regular of type 2 if and only if $3ad + bc \neq 0$. For a fixed non-zero element $a \in \mathbf{F}_q$ we may choose $b, c \in \mathbf{F}_q$ freely and then d cannot equal $-\frac{bc}{3a} \in \mathbf{F}_q$. Hence there are $q^2(q-1)^2$ regular elements of type 2 contained in $C_{\mathfrak{sl}}(x)$. Using Table 5.2, we see that these regular elements correspond to $\frac{q^2(q-1)^2}{(q-1)^2} = q^2$ subspaces $C_{\mathfrak{sl}}(z)$ of $C_{\mathfrak{sl}}(x)$ with z regular of type 2.

- Suppose $z = \left(\begin{smallmatrix} a & b & d \\ 0 & -2a & c \\ 0 & 0 & a \end{smallmatrix}\right) \in C_{\mathfrak{sl}}(x)$ is a regular element of type 3. Then the eigenvalues of z are all zero, hence $a = 0$, and the minimal polynomial of z is given by $T^3 \in \mathbf{F}_q[T]$. We see that z being regular of type 3 is equivalent to $z^2 \neq 0$. We compute

$$z^2 = \left(\begin{smallmatrix} 0 & 0 & bc \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$$

  and hence z is regular of type 3 if and only if $bc \neq 0$. Since we can choose d freely, this shows that there are $q(q-1)^2$ regular elements of type 3 in $C_{\mathfrak{sl}}(x)$. Using Table 5.2, we see that these regular elements correspond to $\frac{q(q-1)^2}{q(q-1)} = q - 1$ subspaces $C_{\mathfrak{sl}}(z)$ of $C_{\mathfrak{sl}}(x)$ with z regular of type 3.

We conclude that $C_{\mathfrak{sl}}(x)$ contains

$$2(q+1) + q^2 + (q-1) = q^2 + 3q + 1$$

two-dimensional subspaces V' satisfying $\dim\left[\mathfrak{sl}_3(\mathbf{F}_q), V'\right] = 6$. Hence the number of two-dimensional subspaces $V \subseteq C_{\mathfrak{sl}}(x)$ with $\dim\left[\mathfrak{sl}_3(\mathbf{F}_q), V\right] = 7$ equals

$$\binom{4}{2}_q - (q^2 + 3q + 1). \tag{5.35}$$

The second case we need to consider, is when x is of type 5; then without loss of generality $x = \left(\begin{smallmatrix} 1 & & \\ & 1 & \\ & & -2 \end{smallmatrix}\right)$. In which case we have

$$C_{\mathfrak{sl}}(x) = \left(\begin{smallmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & * \end{smallmatrix}\right) \cap \mathfrak{sl}_3(\mathbf{F}_q). \tag{5.36}$$

Two-dimensional subspaces $V' \subseteq C_{\mathfrak{sl}}(x)$ with $\dim\left[\mathfrak{sl}_3(\mathbf{F}_q), V'\right] = 6$ come in two flavours: V' is a toxic subspace or V' contains a regular element. We start by calculating the number of two-dimensional toxic subspaces of $C_{\mathfrak{sl}}(x)$.

- Assume V' is a two-dimensional toxic subspace of $C_{\mathfrak{sl}}(x)$. By Theorem 5.6.4 we have $V' = \varphi(UW^T)$ or $V' = \varphi(WU^T)$ for unique subspaces $U, W \subseteq \mathbf{F}_q^3$ with $\dim U = 2$ and $\dim W = 1$. Without loss of generality we assume $V' = \varphi(UW^T)$, the calculation for the other case goes analogously and the end result is the same. Any toxic element in $C_{\mathfrak{sl}}(x)$ can be uniquely written as $\lambda I + y$ for some scalar $\lambda \in \mathbf{F}_q$ and some matrix $y \in \mathfrak{gl}_3(\mathbf{F}_q)$ of rank 1. From the explicit description in (5.36) we deduce that y is contained in
$$\begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & * \end{pmatrix}. \tag{5.37}$$
Note that the row, respectively column, space of a non-zero element from the left space in (5.37) never equals the row, respectively column, space of any non-zero element from the right space in (5.37). Together with Lemma 5.6.3, the fact that V' is two-dimensional and that $\operatorname{char} \mathbf{F}_q \neq 3$, we conclude that
$$UW^T \subseteq \begin{pmatrix} * & * & 0 \\ * & * & 0 \\ 0 & 0 & 0 \end{pmatrix}$$
and hence that $U = \langle e_1, e_2 \rangle$ and $W \subseteq \mathbf{F}_q^2 \oplus \{0\}$. This gives $\binom{2}{1}_q = q + 1$ possibilities for W and all of them result in toxic two-dimensional subspaces of $C_{\mathfrak{sl}}(x)$. This shows that there are $2(q+1)$ possibilities for V'.

Next we calculate the number of subspaces of $C_{\mathfrak{sl}}(x)$ which are of the form $C_{\mathfrak{sl}}(z)$ for some regular element $z \in \mathfrak{sl}_3(\mathbf{F}_q)$. By the description in (5.36) any element of $C_{\mathfrak{sl}}(x)$ has at least one eigenvalue in $\mathbf{F}_q$. So any regular element $z \in C_{\mathfrak{sl}}(x)$ is of type 1a, 1b, 2 or 3. Note that, if $z \in C_{\mathfrak{sl}}(x)$ is regular, then $C_{\mathfrak{sl}}(z) = k[z] \subseteq C_{\mathfrak{sl}}(x)$.

- Suppose $z = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & -(a+d) \end{pmatrix} \in C_{\mathfrak{sl}}(x)$ is a regular element of type 1a. The matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is then diagonalisable over $\mathrm{GL}_2(\mathbf{F}_q)$ to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ for $\lambda, \mu \in \mathbf{F}_q$ with $\lambda \neq \mu$. Moreover, the third eigenvalue of z is $-(\lambda + \mu)$, which is different from λ and μ because z is of type 1a. Table 5.5 shows that there are $q^2 + q$ different matrices in $\mathfrak{gl}_2(\mathbf{F}_q)$ which are conjugate to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$. Note that $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \mu & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ are $\mathrm{GL}_2(\mathbf{F}_q)$-conjugate. So the total number of regular elements of type 1a in $C_{\mathfrak{sl}}(x)$ equals $q^2 + q$ multiplied by half of the number of tuples $(\lambda, \mu, -(\lambda + \mu)) \in \mathbf{F}_q^3$ with $\lambda, \mu, -(\lambda + \mu)$ pairwise different. The number of such tuples equals $(q-1)(q-2)$, giving $\frac{1}{2}(q^2+q)(q-1)(q-2)$ different regular elements of type 1a in $C_{\mathfrak{sl}}(x)$. Using Table 5.2, we see that these regular elements correspond to $\frac{(q^2+q)(q-1)(q-2)}{2(q-1)(q-2)} = \frac{1}{2}(q^2+q)$ subspaces $C_{\mathfrak{sl}}(z)$ of $C_{\mathfrak{sl}}(x)$ with z regular of type 1a.
- Suppose $z = \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & -(a+d) \end{pmatrix} \in C_{\mathfrak{sl}}(x)$ is a regular element of type 1b. Then the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is diagonalisable with eigenvalues in $\mathbf{F}_{q^2} \backslash \mathbf{F}_q$. We read off from Table 5.5 that $\mathfrak{gl}_2(\mathbf{F}_q)$ contains $\frac{1}{2}q^2(q-1)^2$ diagonalisable matrices whose eigenvalues lie in $\mathbf{F}_{q^2} \backslash \mathbf{F}_q$.

Hence $C_{\mathfrak{sl}}(x)$ contains $\frac{1}{2}q^2(q-1)^2$ regular elements of type 1b. Using Table 5.2, we see that these regular elements correspond to $\frac{q^2(q-1)^2}{2q(q-1)} = \frac{1}{2}(q^2-q)$ subspaces $C_{\mathfrak{sl}}(z)$ of $C_{\mathfrak{sl}}(x)$ with z regular of type 1b.

- Suppose $z = \left(\begin{smallmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & -(a+d) \end{smallmatrix}\right) \in C_{\mathfrak{sl}}(x)$ is a regular element of type 2. Then the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is $\mathrm{GL}_2(\mathbf{F}_q)$-conjugate to a 2×2-Jordan block. We read off from Table 5.5 that $\mathfrak{gl}_2(\mathbf{F}_q)$ contains $(q-1)(q^2-1)$ matrices which are conjugate to a 2×2-Jordan block with a non-zero eigenvalue. Hence $C_{\mathfrak{sl}}(x)$ contains $(q-1)(q^2-1)$ regular elements of type 2. Using Table 5.2, we see that these regular elements correspond to $\frac{(q-1)(q^2-1)}{(q-1)^2} = q+1$ subspaces $C_{\mathfrak{sl}}(z)$ of $C_{\mathfrak{sl}}(x)$ with z regular of type 2.

- Suppose $z = \left(\begin{smallmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & -(a+d) \end{smallmatrix}\right) \in C_{\mathfrak{sl}}(x)$ is a regular element of type 3. Since type 3 implies that all eigenvalues are zero, we have $a+d=0$. This shows that the maximum size of a Jordan block of z is 2, which contradicts the fact that z is of type 3 (i.e. z has a Jordan block of size 3). So $C_{\mathfrak{sl}}(x)$ does not contain any regular element of type 3.

We conclude that $C_{\mathfrak{sl}}(x)$ contains

$$2(q+1) + \tfrac{1}{2}(q^2+q) + \tfrac{1}{2}(q^2-q) + q + 1 = q^2 + 3q + 3$$

two-dimensional subspaces V' satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = 6$. Hence the number of two-dimensional subspaces $V \subseteq C_{\mathfrak{sl}}(x)$ with $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$ equals

$$\binom{4}{2}_q - (q^2+3q+3). \tag{5.38}$$

The statement of the lemma now follows from combining (5.35), (5.38) with Lemma 5.6.20.

□

Lemma 5.6.26. *Let $\mathbf{F}_q$ be the finite field of cardinality q with* char $\mathbf{F}_q \notin \{2,3\}$. *There are*

$$(q^2+q+1)(q+1)\left(\binom{4}{2}_q - (q^2+3q+1)\right) + (q^2+q+1)q^2\binom{3}{2}_q$$

two-dimensional subspaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ satisfying the two conditions$\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$ *and* $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$.

Proof. Let $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ be a two-dimensional subspace satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$. Then by Lemma 5.6.17 we have $V \subseteq C_{\mathfrak{sl}}(x)$ for some toxic $x \in \mathfrak{sl}_3(\mathbf{F}_q)$. If additionally $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$, then we must have $V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$. This gives

$$V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V] \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), C_{\mathfrak{sl}}(x)] = (\mathbf{F}_q \cdot x)^{\perp}.$$

Type	Number of orbits	Size of each orbit
$\begin{pmatrix}\lambda & 0\\ 0 & \lambda\end{pmatrix}$	q	1
$\begin{pmatrix}\lambda & 1\\ 0 & \lambda\end{pmatrix}$	q	q^2-1
$\begin{pmatrix}\lambda & 0\\ 0 & \mu\end{pmatrix}, \lambda\neq\mu$	$\frac{q(q-1)}{2}$	q^2+q
$\begin{pmatrix}\lambda & \mu\alpha\\ \mu & \lambda\end{pmatrix}, \mu\neq 0$	$\frac{q(q-1)}{2}$	q^2-q

Table 5.5: Let q be an odd prime power, $\lambda,\mu\in\mathbf{F}_q$ and α a generator for $\mathbf{F}_q^*$. The group $\mathrm{GL}_2(\mathbf{F}_q)$ acts by conjugation on $\mathfrak{gl}_2(\mathbf{F}_q)$. This table displays for each type of matrix in $\mathfrak{gl}_2(\mathbf{F}_q)$ (i.e. up to conjugation: multiple of the identity, 2×2 Jordan block, diagonalisable with different eigenvalues in $\mathbf{F}_q$, respectively $\mathbf{F}_{q^2}\backslash\mathbf{F}_q$) the number of different orbits of that type and the size of each orbit. This is the same table as [2, Table 3.1].

We consider the same case distinction as in the proof of Lemma 5.6.25: x is of type 4 or 5.

Suppose x is of type 4, without loss of generality we may assume that $x=\left(\begin{smallmatrix}0&0&1\\0&0&0\\0&0&0\end{smallmatrix}\right)$. One verifies that

$$C_{\mathfrak{sl}}(x)=\left\{\left(\begin{smallmatrix}a&*&*\\0&-2a&*\\0&0&a\end{smallmatrix}\right)\mid a\in\mathbf{F}_q\right\}\subseteq\left(\begin{smallmatrix}*&*&*\\*&*&*\\0&*&*\end{smallmatrix}\right)\cap\mathfrak{sl}_3(\mathbf{F}_q)=(\mathbf{F}_q\cdot x)^\perp=[\mathfrak{sl}_3(\mathbf{F}_q),C_{\mathfrak{sl}}(x)].$$

Hence for any two-dimensional subspace $V'\subseteq C_{\mathfrak{sl}}(x)$ with $\dim[\mathfrak{sl}_3(\mathbf{F}_q),V']=7$ we have

$$V'+[\mathfrak{sl}_3(\mathbf{F}_q),V']\subseteq C_{\mathfrak{sl}}(x)+[\mathfrak{sl}_3(\mathbf{F}_q),C_{\mathfrak{sl}}(x)]\subseteq[\mathfrak{sl}_3(\mathbf{F}_q),C_{\mathfrak{sl}}(x)]=(\mathbf{F}_q\cdot x)^\perp.$$

Since $\dim(\mathbf{F}_q\cdot x)^\perp=7$ it follows that $\dim V'+[\mathfrak{sl}_3(\mathbf{F}_q),V']=7$ as well. Together with Lemma 5.6.20 and (5.35) this gives

$$(q^2+q+1)(q+1)\left(\binom{4}{2}_q-(q^2+3q+1)\right)$$

two-dimensional spaces $V\subseteq\mathfrak{sl}_3(\mathbf{F}_q)$ satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q),V]=\dim V+[\mathfrak{sl}_3(\mathbf{F}_q),V]=7$ and $V\subseteq C_{\mathfrak{sl}}(z)$ for some toxic element $z\in\mathfrak{sl}_3(\mathbf{F}_q)$ of type 4.

Assume x is of type 5, then without loss of generality we may assume that $x=\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&-2\end{smallmatrix}\right)$. If $V\subseteq C_{\mathfrak{sl}}(x)$ is a two-dimensional subspace satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q),V]=\dim V+[\mathfrak{sl}_3(\mathbf{F}_q),V]=7$, then V satisfies

$$\begin{aligned}V\subseteq C_{\mathfrak{sl}}(x)\cap(\mathbf{F}_q\cdot x)^\perp&=\left(\begin{smallmatrix}*&*&0\\*&*&0\\0&0&*\end{smallmatrix}\right)\cap\left\{\left(\begin{smallmatrix}a&*&*\\*&-a&*\\*&*&0\end{smallmatrix}\right)\mid a\in\mathbf{F}_q\right\}\\&=\left\{\left(\begin{smallmatrix}a&*&0\\*&-a&0\\0&0&0\end{smallmatrix}\right)\mid a\in\mathbf{F}_q\right\}.\end{aligned}$$

Next we show that any two-dimensional subspace V' of the latter space, which we denote by W, satisfies $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = \dim V' + [\mathfrak{sl}_3(\mathbf{F}_q), V'] = 7$. We do this by showing that there are no two-dimensional subspaces V' of W which satisfy $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V'] = 6$. We follow the case distinction of Lemma 5.6.25 in the case of $x = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{smallmatrix}\right)$.

- Suppose V' is a two-dimensional toxic subspace, then by the proof of Lemma 5.6.25 we have $V' = \varphi(UW^T)$ or $V' = \varphi(WU^T)$ with $U = \langle e_1, e_2 \rangle$ and $W \subseteq \mathbf{F}_q^2 \oplus \{0\}$ a one-dimensional subspace. Without loss of generality we may assume $V' = \varphi(UW^T)$, the other case goes analogously. Let $(w_1, w_2, 0) \in W$ be some element, then for all $\lambda, \mu \in \mathbf{F}_q$ we have

$$\begin{pmatrix} \lambda w_1 & \lambda w_2 & 0 \\ \mu w_1 & \mu w_2 & 0 \\ 0 & 0 & 0 \end{pmatrix} - \tfrac{\lambda w_1 + \mu w_2}{3} I = \varphi\left(\begin{pmatrix} \lambda \\ \mu \\ 0 \end{pmatrix} \begin{pmatrix} w_1 & w_2 & 0 \end{pmatrix}\right) \in V'$$

  and hence $\lambda w_1 + \mu w_2 = 0$. Since λ, μ were arbitrary, it follows that $w_1 = w_2 = 0$, a contradiction. So W does not contain two-dimensional toxic subspaces.

- Suppose $z = \left(\begin{smallmatrix} a & b & 0 \\ c & -a & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in V'$ is a regular element with $C_{\mathfrak{sl}}(z) \subseteq W$. We compute

$$\begin{pmatrix} a^2+bc & 0 & 0 \\ 0 & a^2+bc & 0 \\ 0 & 0 & 0 \end{pmatrix} - \tfrac{2(a^2+bc)}{3} I = z^2 - \tfrac{\operatorname{Tr}(z^2)}{3} I \in W$$

  and by looking at the bottom right entry, we find that $a^2 + bc = 0$. It follows that $z^2 = 0$, which gives a contradiction with z being regular.

Together with Lemma 5.6.20 this gives

$$(q^2 + q + 1)q^2 \binom{3}{2}_q$$

two dimensional spaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ satisfying $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = \dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$ and $V \subseteq C_{\mathfrak{sl}}(z)$ for some toxic element $z \in \mathfrak{sl}_3(\mathbf{F}_q)$ of type 5. □

The cases $\dim V \in \{3, 4\}$

For $\delta_K \in \{0, 1\}$ and three-dimensional or four-dimensional subspaces $V \subseteq \mathfrak{sl}_d(\mathbf{F}_q)$ we investigate the map

$$V \mapsto \delta_K V + [\mathfrak{sl}_3(\mathbf{F}_q), V].$$

Lemma 5.6.27. *Let $\mathbf{F}_q$ be the finite field of cardinality q with* $\operatorname{char} \mathbf{F}_q \notin \{2, 3\}$. *Let $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ be a subspace of dimension* $\dim V = \ell \in \{3, 4\}$ *satisfying* $\dim[\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$.

(a) When

- $\ell = 3$, *we have* $\binom{4}{3}_q \cdot (q^2+q+1)^2$ *such subspaces* V*;*
- $\ell = 4$, *we have* $(q^2+q+1)^2$ *such subspaces* V*.*

(b) When the subspace V *satisfies the additionally* $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$*, then if*

- $\ell = 3$, *we have* $(q^2+q+1)\left(q^2 + (q+1)\binom{4}{3}_q\right)$ *such subspaces* V*;*
- $\ell = 4$, *we have* $(q^2+q+1)(q+1)$ *such subspaces* V*.*

Proof. By Lemma 5.6.17 there exists a unique one-dimensional toxic subspace U such that $V \subseteq C_{\mathfrak{sl}}(U)$. Let $z \in U$ be a non-zero element; by Lemma 5.4.2 and Theorem 5.4.4 we have

$$[\mathfrak{sl}_3(\mathbf{F}_q), V] \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), C_{\mathfrak{sl}}(U)] = C_{\mathfrak{sl}}(C_{\mathfrak{sl}}(z))^\perp = (\mathbf{F}_q \cdot z)^\perp. \tag{5.39}$$

Because $\dim (\mathbf{F}_q \cdot z)^\perp = 7$, it follows that we have the equality $[\mathfrak{sl}_3(\mathbf{F}_q), V] = (\mathbf{F}_q \cdot z)^\perp$. Conversily, if $W \subseteq C_{\mathfrak{sl}}(U)$ is an ℓ-dimensional subspace, then similarly $[\mathfrak{sl}_3(\mathbf{F}_q), W] \subseteq (\mathbf{F}_q \cdot z)^\perp$ and hence $\dim [\mathfrak{sl}_3(\mathbf{F}_q), W] \leq 7$. Together with Lemma 5.6.16 this shows $\dim [\mathfrak{sl}_3(\mathbf{F}_q), W] = 7$.

The above shows that for every one-dimensional toxic subspaces $U \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ we have $\binom{4}{\ell}_q$ subspaces $V \subseteq C_{\mathfrak{sl}}(U)$ with $\dim V = \ell$ satisfying $\dim [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$. From Lemma 5.6.20 it follows that there are precisely $(q^2+q+1)^2$ such subspaces U. Part (a) now follows.

For part (b) note that $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$ if and only if $V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$. We perform a case distinction depending upon the type of z.

- Assume $z = \left(\begin{smallmatrix} 0 & 0 & 1 \\ & 0 & \\ & & 0 \end{smallmatrix}\right)$, then we have

  $$C_{\mathfrak{sl}}(z) = \left\{ \left(\begin{smallmatrix} a & * & * \\ & -2a & * \\ & & a \end{smallmatrix}\right) \mid a \in \mathbf{F}_q \right\} \quad \text{and} \quad (\mathbf{F}_q \cdot z)^\perp = \left(\begin{smallmatrix} * & * & * \\ * & * & * \\ 0 & * & * \end{smallmatrix}\right) \cap \mathfrak{sl}_3(\mathbf{F}_q).$$

  From the observation following (5.39) any subspace $W \subseteq C_{\mathfrak{sl}}(z)$ with $\dim W = \ell$ satisfies $W \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), W]$. Lemma 5.6.20 tells us that there are $(q^2+q+1)(q+1)$ toxic subspaces of $\mathfrak{sl}_3(\mathbf{F}_q)$ such that every non-zero element has type 4. This case gives us $\binom{4}{\ell}_q \cdot (q^2+q+1)(q+1)$ subspaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ of dimension $\dim V = \ell$ satisfying $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$.

- Assume $z = \left(\begin{smallmatrix} 1 & & \\ & 1 & \\ & & -2 \end{smallmatrix}\right)$; then we have

  $$C_{\mathfrak{sl}}(z) = \left(\begin{smallmatrix} * & * & \\ * & * & \\ & & * \end{smallmatrix}\right) \cap \mathfrak{sl}_3(\mathbf{F}_q) \quad \text{and} \quad (\mathbf{F}_q \cdot z)^\perp = \left\{ \left(\begin{smallmatrix} a & * & * \\ * & -a & * \\ * & * & 0 \end{smallmatrix}\right) \mid a \in k \right\}.$$

Because the subspace V satisfies $V \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), V]$, we have $V \subseteq C_{\mathfrak{sl}}(z) \cap (\mathbf{F}_q \cdot z)^\perp$. We compute

$$V \subseteq \begin{pmatrix} * & * & \\ * & * & \\ & & * \end{pmatrix} \cap \left\{ \begin{pmatrix} a & * & * \\ * & -a & * \\ * & * & 0 \end{pmatrix} \mid a \in \mathbf{F}_q \right\} = \left\{ \begin{pmatrix} a & * & \\ * & -a & \\ & & \end{pmatrix} \mid a \in \mathbf{F}_q \right\}.$$

The latter space is three-dimensional, so $\dim V = 3$ and we have equality. A straightforward verification shows that the subspace $W = \left\{ \begin{pmatrix} a & * & \\ * & -a & \\ & & \end{pmatrix} \mid a \in \mathbf{F}_q \right\}$ indeed satisfies $W \subseteq C_{\mathfrak{sl}}(z)$ and $W \subseteq [\mathfrak{sl}_3(\mathbf{F}_q), W]$. By Lemma 5.6.20 there are $(q^2+q+1)q^2$ one-dimensional toxic subspaces with every non-zero element of type 5. Hence this case gives us $(q^2+q+1)q^2$ subspaces $V \subseteq \mathfrak{sl}_3(\mathbf{F}_q)$ of dimension $\dim V = 3$ satisfying $\dim V + [\mathfrak{sl}_3(\mathbf{F}_q), V] = 7$. □

5.6.5 Calculations for $\mathfrak{sl}_2$

Let k be a field with char $k \neq 2$ and write $L = \mathfrak{sl}_2(k)$. We show for a subspace $V \subseteq L$ how the dimension of $[V, L]$ depends upon V. Recall that for a non-zero element $x \in L$ we have $C_{\mathfrak{sl}}(x) = \langle x \rangle$.

For $V = 0$ we have $[0, L] = 0$. Let $x \in L$ be a non-zero element, by Lemma 5.4.2 we compute for the one-dimensional vector space $V = \langle x \rangle$ that

$$\dim [V, L] = \dim C_{\mathfrak{sl}}(V)^\perp = \dim L - \dim C_{\mathfrak{sl}}(\langle x \rangle) = 3 - 1 = 2.$$

Moreover, for two linearly independent elements $x, y \in L$ we find similarly by Lemma 5.4.2 for the two-dimensional space $V = \langle x, y \rangle$ that

$$\dim [V, L] = \dim L - \dim C_{\mathfrak{sl}}(\langle x, y \rangle) = 3,$$

using $C_{\mathfrak{sl}}(\langle x, y \rangle) = C_{\mathfrak{sl}}(\langle x \rangle) \cap C_{\mathfrak{sl}}(\langle y \rangle) = \langle x \rangle \cap \langle y \rangle = 0$. When $V = L$ we have $[V, L] = L$, because V contains a two-dimensional subspace. This shows for a subspace $V \subseteq L$ that the dimension of $[V, L]$ is completely determined by the dimension of V.

Next we show for a subspace $V \subseteq L$ how the dimension of the vector space $V + [L, V]$ depends upon V. From the discussion above we see for a subspace $V \subseteq L$ with $\dim V \geq 2$ we always have $[V, L] = L$. Therefore we only need to consider the case where V is one-dimensional.

Suppose $V = \langle x \rangle$ for some non-zero $x \in L$. Since $\dim [V, L] \geq 2$ and $\dim L = 3$ we have that $\dim V + [V, L] = 2$ holds if and only if $V \subseteq [V, L]$. The condition $V \subseteq [V, L]$ is the same as $\langle x \rangle \subseteq \langle x \rangle^\perp$, which is in turn equivalent to $\kappa(x, x) = 0$. Because the characteristic

of k is not 2, it follows from $\kappa(x,x) = 4\mathrm{Tr}(x^2)$ that $\mathrm{Tr}(x^2) = 0$. The Cayley-Hamilton theorem shows that the element x satisfies

$$x^2 - \mathrm{Tr}(x)x + \det(x)I = 0$$

and by taking the trace of this formula we see that $\mathrm{Tr}(x^2) - \mathrm{Tr}(x)^2 + 2\det(x) = 0$. Because $\mathrm{Tr}(x^2) = \mathrm{Tr}(x) = 0$ this gives $\det(x) = 0$, using again that char $k \neq 2$. We conclude that $V \subseteq [V,L]$ holds if and only if $\det(x) = 0$.

Let $k = \mathbf{F}_q$, the field with q elements, and suppose that char $k \neq 2$. We count the number of one-dimensional subspaces $V \subseteq L$ satisfying $\dim V + [V,L] = 2$. We can write any element of L as a matrix $\left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$ with $a,b,c \in k$. This matrix has determinant zero if $a^2+bc = 0$. The number of non-zero triples $(a,b,c) \in k^3$ satisfying $a^2+bc = 0$ equals q^2-1. Namely, if $b = 0$ then $a = 0$ and so c is non-zero, giving $q-1$ possibilities; and if $b \neq 0$ then for any choice of a the value of c is determined, giving the remaining $(q-1)q$ possibilities. Every one-dimensional subspace of L contains $q-1$ different non-zero elements, hence the number of one-dimensional subspace $V \subseteq L$ satisfying $\dim V + [V,L] = 2$ equals

$$\frac{q^2-1}{q-1} = q+1.$$

As the total number of one-dimensional subspaces of L equals q^2+q+1 we see that there are q^2 one-dimensional subspaces $V \subseteq L$ with $V + [V,L] = L$.

5.6.6 Normal zeta functions for $\mathbf{SL}_2$

Using the results from Section 5.6.5 we compute the normal zeta functions of the groups $\mathrm{SL}_2^1(\mathbf{F}_p[\![t]\!])$ and $\mathrm{SL}_2^1(\mathbf{Z}_p)$ for prime numbers $p > 2$.

The group $\mathbf{SL}_2^1(\mathbf{F}_p[\![t]\!])$

Let $p > 2$ be a prime number and write $G = \mathrm{SL}_2^1(\mathbf{F}_p[\![t]\!])$. The Lie algebra we need to consider is $L = \mathfrak{sl}_2(\mathbf{F}_p)$ of size p^3. The normal zeta function $\zeta_G^{\triangleleft}(s)$ is given by the general formula from Theorem 5.1.2:

$$\zeta_G^{\triangleleft}(s) = \frac{1}{1-p^{-3s}} \sum_{0 \neq V \subseteq L} |L:V|^{-s} \left(\sum_{[V,L] \subseteq W \subseteq L} |L:W|^{-s+\dim V} \right),$$

where V, W are subspaces of L. We first calculate the inner sum according to the dimension of V.

Suppose $\dim V = 1$, then $[V, L]$ is two-dimensional and hence W equals either $[V, L]$ or L in which case $|L : W|$ equals p or 1, respectively. It follows that the inner sum equals

$$p^{-s+1} + 1.$$

Suppose $\dim V \in \{2, 3\}$, then $[V, L] = L$ so that $W = L$ and hence the inner sum equals 1. The numbers of one-dimensional and two-dimensional subspaces of L both equal p^2+p+1. Therefore, the normal zeta function for G is given by

$$\begin{aligned}\zeta_G^{\triangleleft}(s) &= \frac{(p^2+p+1)p^{-2s}(p^{-s+1}+1) + (p^2+p+1)p^{-s} + 1}{1-p^{-3s}} \\ &= \frac{1 + (p^2+p+1)(p^{-s}+p^{-2s}+p\cdot p^{-3s})}{1-p^{-3s}}.\end{aligned}$$

The group $\mathbf{SL}_2^1(\mathbf{Z}_p)$

Let $p > 2$ be a prime number and write $G = \mathrm{SL}_2^1(\mathbf{Z}_p)$. The Lie algebra we need to consider is $L = \mathfrak{sl}_2(\mathbf{F}_p)$ of size p^3. The normal zeta function $\zeta_G^{\triangleleft}(s)$ is given by the formula from Theorem 5.1.2:

$$\zeta_G^{\triangleleft}(s) = \frac{1}{1-p^{-3s}} \sum_{0 \neq V \subseteq L} |L : V|^{-s} \left(\sum_{V+[V,L] \subseteq W \subseteq L} |L : W|^{-s+\dim V} \right),$$

where V, W are subspaces of L. We first calculate the inner sum according to the dimension of V.

Suppose $\dim V = 1$ and $\dim V + [V, L] = 2$; then W equals either $[V, L]$ or L in which case $|L : W|$ equals p or 1 respectively. It follows that the inner sum equals

$$p^{-s+1} + 1.$$

Suppose $\dim V = 1$ and $\dim V + [V, L] = 3$ or $\dim V \in \{2, 3\}$, then $W = L$ and hence the inner sum equals 1. The number of one-dimensional subspaces $V \subseteq L$ with $\dim V + [V, L] = 2$ equals $p + 1$ and the number of one-dimensional subspaces $V \subseteq L$ with $V + [V, L] = L$ equals p^2. The number of two dimensional subspaces of L equals $p^2 + p + 1$. Therefore, the normal zeta function for G is given by

$$\begin{aligned}\zeta_G^{\triangleleft}(s) &= \frac{(p+1)p^{-2s}(p^{-s+1}+1) + p^2\cdot p^{-2s} + (p^2+p+1)p^{-s} + 1}{1-p^{-3s}} \\ &= \frac{1 + (p^2+p+1)(p^{-s}+p^{-2s}) + (p^2+p)\cdot p^{-3s}}{1-p^{-3s}} \\ &= \frac{1 + p\cdot p^{-s} + p^2\cdot p^{-s}}{1-p^{-s}} = 1 + \frac{(p^2+p+1)p^{-s}}{1-p^{-s}}.\end{aligned}$$

5.6.7 Normal zeta functions for SL_3

For a prime number $p > 3$ let G be the group $\mathrm{SL}_3^1(\mathbf{F}_p[\![T]\!])$ or $\mathrm{SL}_3^1(\mathbf{Z}_p)$. We compute the normal zeta function $\zeta_G^{\triangleleft}(s)$ of G using Theorem 5.1.2 together with the results from Section 5.6.4. In Section 5.6.4 we computed for all integers $1 \leq m, n \leq 8$ the number $g(m,n)$ of m-dimensional subspaces V of $L = \mathfrak{sl}_3(\mathbf{F}_p)$ with $n = \dim_{\mathbf{F}_p}(\delta_K V + [L,V])$. For such a subspace V the inner summation in Theorem 5.1.2 is given by

$$\sum_{\delta_K V + [L,V] \subseteq W \subseteq L} |L : W|^{-s+\dim_{\mathbf{F}_p} V} = \sum_{i=n}^{8} \binom{8-n}{i-n}_p \left(p^{8-i}\right)^{-s+m}.$$

For integers $1 \leq m, n \leq 8$ the contribution of all m-dimensional subspaces V of L with $n = \dim_{\mathbf{F}_p}(\delta_K V + [L,V])$ to $(1-t^8)\zeta_G^{\triangleleft}(s)$, here $t = p^{-s}$, is therefore

$$g(m,n) t^{8-m} \sum_{i=n}^{8} \binom{8-n}{i-n}_p p^{(8-i)m} t^{8-i}. \tag{5.40}$$

Summing these contributions for all $1 \leq m, n \leq 8$ lets us compute $\zeta_G^{\triangleleft}(s)$ explicitly.

The group $\mathbf{SL}_3^1(\mathbf{F}_p[\![T]\!])$

For the group $G = \mathrm{SL}_3^1(\mathbf{F}_p[\![T]\!])$ we have $\delta_K = 0$, because $K = \mathbf{F}_p(\!(T)\!)$. If (m,n) is a pair of integers with $1 \leq m, n \leq 8$ for which there exists an m-dimensional subspace V of L satisfying $n = \dim [L,V]$, then

$$(m,n) \in \{(1,4),(1,6),(2,6),(2,7),(3,7),(4,7)\} \cup \{(m,8) \mid 2 \leq m \leq 8\}.$$

By Lemma 5.6.22(b) we have

$$g(1,4) = (p^2+p+1)^2 \quad \text{and} \quad g(1,6) = \binom{8}{1}_p - (p^2+p+1)^2.$$

From Lemma 5.6.23(b) and Lemma 5.6.24(a) we deduce that

$$g(2,6) = 2(p^2+p+1)^2 + (p^6+p^5+3p^4+3p^3+p^2-p-1).$$

Lemma 5.6.25 shows that

$$g(2,7) = (p^2+p+1)(p^6+2p^5+3p^4-3p^2-2p)$$

and consequently we have $g(2,8) = \binom{8}{2}_p - g(2,6) - g(2,7)$. Lemma 5.6.27(a) gives

$$g(3,7) = \binom{4}{3}_p (p^2+p+1)^2$$

and hence $g(3,8) = \binom{8}{3}_p - g(3,7)$. Using Lemma 5.6.27(a) we see that

$$g(4,7) = (p^2+p+1)^2$$

and hence $g(4,8) = \binom{8}{4}_p - g(4,7)$. Finally we have $g(m,8) = \binom{8}{m}_p$ for $5 \leq m \leq 8$. This gives

$$\begin{aligned}(1-t^8)\zeta_G^{\triangleleft}(s) = 1 &+ \binom{8}{7}_p t + \binom{8}{6}_p t^2 + \binom{8}{5}_p t^3 + \binom{8}{4}_p t^4 + \left(\binom{8}{3}_p + g(4,7)p^4\right) t^5 \\ &+ \left(\binom{8}{2}_p + g(3,7)p^3\right) t^6 + \left(\binom{8}{1}_p + g(2,7)p^2 + g(2,6)p^2\binom{2}{1}_p\right) t^7 \\ &+ \left(g(2,6)p^4 + \left(\binom{8}{1}_p - g(1,4)\right)p\binom{2}{1}_p + g(1,4)p\binom{4}{1}_p\right) t^8 \\ &+ \left(\left(\binom{8}{1}_p - g(1,4)\right)p^2 + g(1,4)p^2\binom{4}{2}_p\right) t^9 + g(1,4)p^3\binom{4}{1}_p t^{10} \\ &+ g(1,4)p^4 t^{11}\end{aligned}$$

Consequently, the normal zeta function $\zeta^{\triangleleft}_{\mathrm{SL}_3^1(\mathbf{F}_p[\![T]\!])}(s)$ of the group $\mathrm{SL}_3^1(\mathbf{F}_p[\![T]\!])$ is of the form

$$\frac{a_0(p) + a_1(p)t + a_2(p)t^2 + \ldots + a_{11}(p)t^{11}}{1-t^8},$$

where $a_i(X) \in \mathbf{Z}[X]$ for $0 \leq i \leq 11$ are polynomials, by a routine but somewhat tedious calculation. Explicitly we have $a_i(p) = \binom{8}{i}_p$ for $0 \leq i \leq 4$ (so $a_0(p) = 1$), $a_5(p) = \binom{8}{5}_p + (p^2+p+1)^2p^4$, $a_6(p) = \binom{8}{2}_p + p^3(p^2+p+1)^2\binom{4}{3}_p$, $a_{10}(p) = \binom{4}{1}_p(p^2+p+1)^2p^3$ and $a_{11}(p) = (p^2+p+1)^2p^4$. Furthermore we have

$$\begin{aligned}a_7(p) &= p^{10} + 4p^9 + 8p^8 + 12p^7 + 13p^6 + 10p^5 + 6p^4 + 3p^3 + 2p^2 + p + 1 \\ a_8(p) &= p^{10} + 2p^9 + 8p^8 + 12p^7 + 14p^6 + 10p^5 + 6p^4 + 3p^3 + 2p^2 + p \\ a_9(p) &= p^{10} + 4p^9 + 8p^8 + 11p^7 + 12p^6 + 9p^5 + 5p^4 + 2p^3 + p^2.\end{aligned}$$

The group $\mathbf{SL}_3^1(\mathbf{Z}_p)$

For the group $G = \mathrm{SL}_3^1(\mathbf{Z}_p)$ we have $\delta_K = 1$, because $K = \mathbf{Q}_p$. If (m,n) is a pair of integers with $1 \leq m,n \leq 8$ for which there exists an m-dimensional subspace V of L satisfying $n = \dim[L,V]$, then

$$(m,n) \in \{(1,4),(1,5),(1,6),(1,7),(2,6),(2,7),(3,7),(4,7)\} \cup \{(m,8) \mid 2 \leq m \leq 8\}.$$

By Lemma 5.6.22(c) we have

$$g(1,4) = (p^2+p+1)(p+1), \quad g(1,5) = (p^2+p+1)p^2, \quad g(1,6) = (p^3-1)(p^2+p)$$

and consequently $g(1,7) = \binom{8}{1}_p - g(1,4) - g(1,5) - g(1,6)$. Using Lemma 5.6.23(c), Lemma 5.6.24(b) and Lemma 5.6.26 we have

$$g(2,6) = 2(p^2+p+1) + (p^3-1)(p+1)$$

and

$$g(2,7) = (p^2+p+1)(p^5+3p^4+4p^3+3p^2),$$

consequently we have $g(2,8) = \binom{8}{2}_p - g(2,6) - g(2,7)$. It follows from Lemma 5.6.27(b) that

$$g(3,7) = (p^2+p+1)\left(p^2 + (p+1)\binom{4}{3}_p\right)$$

and hence $g(3,8) = \binom{8}{3}_p - g(3,7)$. Using Lemma 5.6.27(b) we see that

$$g(4,7) = (p^2+p+1)(p+1)$$

and hence $g(4,8) = \binom{8}{4}_p - g(4,7)$. Finally we have $g(m,8) = \binom{8}{m}_p$ for $5 \le m \le 8$. This gives

$$\begin{aligned}(1-t^8)\zeta_G^{\triangleleft}(s) = 1 &+ \binom{8}{7}_p t + \binom{8}{6}_p t^2 + \binom{8}{5}_p t^3 + \binom{8}{4}_p t^4 + \left(\binom{8}{3}_p + g(4,7)p^4\right)t^5 \\ &+ \left(\binom{8}{2}_p + g(3,7)p^3\right)t^6 + \left(\binom{8}{1}_p + g(2,7)p^2 + g(2,6)p^2\binom{2}{1}_p\right)t^7 \\ &+ \left(g(1,4)p\binom{4}{3}_p + g(1,5)p\binom{3}{2}_p + g(1,6)p\binom{2}{1}_p + g(1,7)p + g(2,6)p^4\right)t^8 \\ &+ \left(g(1,4)p^2\binom{4}{2}_p + g(1,5)p^2\binom{3}{1}_p + g(1,6)p^2\right)t^9 \\ &+ \left(g(1,4)p^3\binom{4}{1}_p + g(1,5)p^3\right)t^{10} + g(1,4)p^4t^{11}\end{aligned}$$

Consequently, the normal zeta function $\zeta^{\triangleleft}_{\mathrm{SL}_3^1(\mathbf{Z}_p)}(s)$ of the group $\mathrm{SL}_3^1(\mathbf{Z}_p)$ is of the form

$$\frac{b_0(p) + b_1(p)t + b_2(p)t^2 + \ldots + b_{11}(p)t^{11}}{1-t^8},$$

where $b_i(X) \in \mathbf{Z}[X]$ for $0 \le i \le 11$ are polynomials, by a routine but somewhat tedious calculation. Explicitly we have $b_i(p) = \binom{8}{i}_p$ for $0 \le i \le 4$ (so $b_0(p) = 1$), $b_5(p) =$

$\binom{8}{5}_p + (p^2+p+1)(p+1)p^4$ and $b_{11}(p) = (p^2+p+1)(p+1)p^4$. Furthermore we have the following formulas for the remaining $b_i(p)$:

$$\begin{aligned}
b_6(p) &= \binom{8}{2}_p + p^3(p^2+p+1)^3 \\
b_7(p) &= p^9 + 4p^8 + 10p^7 + 13p^6 + 11p^5 + 7p^4 + 3p^3 + 2p^2 + p + 1 \\
b_8(p) &= 2p^8 + 5p^7 + 9p^6 + 9p^5 + 7p^4 + 3p^3 + 2p^2 + p \\
b_9(p) &= p^2(p^2+p+1)(p^5 + 3p^4 + 5p^3 + 4p^2 + p + 1) \\
b_{10}(p) &= p^3(p^2+p+1)^3.
\end{aligned}$$

Bibliography

[1] J.-P. Allouche; J. Shallit; *Automatic sequences*, Cambridge University Press, Cambridge (2003).

[2] N. Avni; B. Klopsch; U. Onn; C. Voll; *Representation zeta functions of compact p-adic analytic groups and arithmetic groups*, Duke Math. J. **162**, no. 1 (2013), 111–197.

[3] Y. Barnea; R. Guralnick; *Subgroup growth in some pro-p groups.* Proc. Amer. Math. Soc. **130** (2002), 653–659.

[4] Y. Barnea; J.-C. Schlage-Puchta; *Large normal subgroup growth and large characteristic subgroup growth*, J. Group Theory **23** (2020), 1–15.

[5] F. M. Bleher; T. Chinburg; B. Poonen; P. Symonds; *Automorphisms of Harbater-Katz-Gabber curves*, Math. Ann. **368** (2017), no. 1-2, 811–836.

[6] S. Bogataya; S. Bogatyi; D. Kiselev; *Powers of elements of the series substitution group* $\mathcal{J}(\mathbb{Z}_2)$, Topology Appl. **201** (2016), 29–56.

[7] W. Borho; *Über Schichten halbeinfacher Lie-Algebren*, Invent. math. **65** (1981), 283–317.

[8] K. Bou-Rabee; D. Studenmund; *Arithmetic lattices in unipotent algebraic groups*, J. Group Theory **23** (2020), no. 2, 299–312.

[9] K. Bou-Rabee; T. Kaletha; D. Studenmund; *Commensurability growths of algebraic groups*, Math. Zeitschrift **294** (2020), 1749–1757.

[10] A. Bridy, *Automatic sequences and curves over finite fields*, Algebra Number Theory **11** (2017), no. 3, 685–712.

[11] F. Bruhat, J. Tits; *Groupes réductifs sur un corps local*, Publ. Math. I.H.E.S. **41** (1972), 1–251.

[12] C. Bushnell; I. Reiner; *Zeta functions of arithmetic orders and Solomon's conjecture*, Math. Z. **173** (1980), 135–161.

[13] J. Byszewski; G. Cornelissen; D. Tijsma (2020), *Automata and finite order elements in the Nottingham group*, arXiv: 2008.04971.

[14] J. Byszewski; G. Cornelissen; D. Tijsma; *Automata and finite order elements in the Nottingham group*, J. Algebra **602** (2022), 484–554.

[15] R. Camina; *Subgroups of the Nottingham group*, J. Algebra **196** (1997), no. 1, 101–113.

[16] T. Chinburg; P. Symonds; *An element of order 4 in the Nottingham group at the prime 2*, preprint arxiv:1009.5135, 3pp., 2010.

[17] A. Cobham; *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192.

[18] D. Collingwood; W. McGovern; *Nilpotent orbits in semisimple Lie algebras*, Van Nostrand Reinhold, New York (1993).

[19] G. Christol; *Ensembles presque periodiques k-reconnaissables*, Theoret. Comput. Sci. **9** (1979), no. 1, 141–145.

[20] G. Christol; T. Kamae; M. Mendès France; G. Rauzy; *Suites algébriques, automates et substitutions*, Bull. Soc. Math. France **108** (1980), no. 4, 401–419.

[21] M. du Sautoy; *The zeta function of* $\mathfrak{sl}_2(\mathbf{Z})$, Forum Math. **12** (2000), 197–221.

[22] M. du Sautoy; L. Woodward; *Zeta functions of groups and rings*, Lecture Notes in Mathematics, **1925**, Springer-Verlag, Berlin (2008).

[23] D. Eisenbud; *Commutative algebra with a view towards algebraic geometry*, Springer-Verlag, New York (1995).

[24] M. Ershov; *New just-infinite pro-p groups of finite width and subgroups of the Nottingham group*, J. Algebra **275** (2004), no. 1, 419–449.

[25] I. Fesenko; *On just infinite pro-p-groups and arithmetically profinite extensions of local fields*, J. Reine Angew. Math. **517** (1999), 61–80.

[26] R. Groot Koerkamp; C++ *program for searching small automata for algebraic power series over* $\mathbf{F}_2$, `https://github.com/RagnarGrootKoerkamp/automata/releases/tag/v1.0` (version released 5 Aug 2020).

[27] F. J. Grunewald; D. Segal; G. C. Smith; *Subgroups of finite index in nilpotent groups* Invent. math. **93** (1988), 185–223.

[28] F. Grunewald; M. du Sautoy; *Analytic properties of zeta functions and subgroup growth*, Ann. Math. **152** (2000), no. 3, 793–833.

[29] M. Hall; *Subgroups of finite index in free groups*, Canadian J. Math. **1** (1949), 187–190.

[30] A. Jaikin-Zapirain; *Zeta function of representations of compact p-adic analytic groups*. J. of the Am. Math. Soc. **19** (2005), no. 1, 91–118.

[31] S. Jean; *Classification à conjugaison près des séries de p-torsion*, `https://www.theses.fr/2008LIMO4011`, (accessed 6 Apr 2018), Doctoral Thesis (108 pp.), Université de Limoges (2008).

[32] S. Jean; *Conjugacy classes of series in positive characteristic and Witt vectors*, J. Théor. Nombres Bordeaux **21** (2009), no. 2, 263–284.

[33] T. Kambayashi; M. Miyanishi; M. Takeuchi; *Unipotent algebraic groups*, Springer-Verlag, Berlin (1974).

[34] D. Kiselev; *Explicit embeddings of finite abelian p-groups in the group* $\mathcal{J}(\mathbb{F}_p)$, Mat. Zametki **97** (2015), no. 1, 74–79.

[35] B. Klopsch; *Automorphisms of the Nottingham group*, J. Algebra **223** (2000), no. 1, 37–56.

[36] B. Klopsch; *Zeta functions related to the pro-p group* $\mathrm{SL}_1(\Delta_p)$, Math. Proc. Camb. Phil. Soc. **135** (2003), 45–57.

[37] B. Klopsch; I. Snopce; *Normal subgroups of Chevalley groups*, in preparation.

[38] W. Knapp; *Lie groups beyond an introduction*, Progr. in Math. **2**, 2nd Edition, Birkhäuser, Boston (2002).

[39] S. Lee; C. Voll; *Zeta functions of integral nilpotent quiver representations*, International Mathematics Research Notices (2021), rnab345, `https://doi.org/10.1093/imrn/rnab345`.

[40] F. Lorenz; *Algebra. Vol. II* (*Fields with structure, algebras and advanced topics*), Universitext, Springer, New York (2008).

[41] J. Lubin; *Torsion in the Nottingham group*, Bull. Lond. Math. Soc. **43** (2011), no. 3, 547–560.

[42] A. Lubotzky; A. Mann; D. Segal; *Finitely generated groups of polynomial subgroup growth*, Israel J. of Math. **82** (1993), 363–371.

[43] A. Lubotzky; A. Mann; *On some* Λ*-analytic pro-p groups*, Isreal J. Math. **85** (1994), 307–337.

[44] A. Lubotzky; *Enumerating boundedly generated finite groups*, J. Algebra **238** (2001), 194–199.

[45] A. Lubotzky; D. Segal; *Subgroup growth*, Progr. in Math. **212**, Birkhäuser Verlag, Basel (2003).

[46] A. Macintyre; *Rationality of p-adic Poincaré series: uniformity in p*, Ann. Pure Appl. Logic **49** (1990), no. 1, 31–74.

[47] A. Mann; *Enumerating finite groups and their defining relations*, J. Group Theory **1** (1998), 59–64.

[48] W. Magnus; *Über Gruppen und zugeordnete Liesche Ringe*, Reine Angew. Math., **182** (1940), 142–159.

[49] B. Mazur; *An introduction to the deformation theory of Galois representations*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York (1997), pp. 243–311.

[50] N. Nikolov; D. Segal; *On finitely generated profinite groups, I: strong completeness and uniform bounds*, Ann. of Math. (2) **165**(1) (2007), 171–238.

[51] O.T. O'Meara; *Introduction to quadratic forms*, Springer-Verlag, Berlin (1973).

[52] V. Platonov; A. Rapinchuk; *Algebraic groups and number theory*, Pure and applied math., **139**, Academic Press, Inc., San Diego (1994).

[53] E. Rowland; R. Yassawi; *Automatic congruences for diagonals of rational functions*, J. Théor. Nombres Bordeaux **27** (2015), no. 1, 245–288.

[54] M. M. Schein; C. Voll; *Normal zeta functions of the Heisenberg groups over number rings I - the unramified case*, J. Lond. Math. Soc. **91** (2014), no. 1, 19–46.

[55] M. M. Schein; C. Voll; *Normal zeta functions of the Heisenberg groups over number rings II - the non-split case*, Israel J. Math. **211** (2016), no. 1, 171–195.

[56] D. Segal; *On the growth of ideals and submodules*, J. London Math. Soc. **56** (1997), no. 2, 245–263.

[57] D. Segal; *Ideals of finite index in a polynomial ring*, Quarterly J. Math. Oxford Ser. **48** (1997), no. 2, 83–92.

[58] I. Snopce; *Normal zeta functions of some pro-p Groups*, Comm. in Algebra, **39** (2011), no. 11, 3969–3980.

[59] J.-P. Serre; *Trees*, Springer-Verlag, Berlin (1980).

[60] A. Shalev; *Lie methods in the theory of pro-p groups* New Horizons in Pro-*p* Groups, Birkhäuser, Basel (2000).

[61] D. Tijsma; *Automata and finite order elements in the Nottingham group*, Master thesis, Utrecht University, `https://dspace.library.uu.nl/handle/1874/366218`, 2018.

[62] C. Voll; *Zeta functions of groups and enumeration in Bruhat-Tits buildings*, Amer. J. Math. **126** (2004), 1005–1032.

[63] C. Voll; *Functional equations for zeta functions of groups and rings*, Ann. of Math. **172** (2010), no. 2, 1181–1218.

Eidesstattliche Erklärung

Ich versichere an Eides statt, dass diese Dissertation von mir selbständig und ohne unzulässige fremde Hilfe unter Beachtung der "Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Univeristät Düsseldorf" erstellt worden ist.

Djurre Tijsma
Düsseldorf, April 2022